UNIVERSITY OF SOUTHAMPTON

Radio Frequency Ranging for Wireless Sensor Network Localization

by

B. Thorbjornsen

A thesis submitted in partial fulfillment for the degree of Doctor of Philosophy

in the

Faculty of Engineering and Applied Science

Department of Electronics and Computer Science

November 2010

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING AND APPLIED SCIENCE
DEPARTMENT OF ELECTRONICS AND COMPUTER SCIENCE

Doctor of Philosophy

by B. Thorbjornsen

Wireless sensor networks (WSNs) have a diverse range of industrial, scientific and medical applications where the sensor nodes are of low cost, standard with respect to hardware architecture, processing abilities and communicate using low-power narrow-band radios. Position information of the sensing nodes within those applications is often a requirement in order to make use of the data recorded by the sensors themselves. On deployment, sensing nodes normally have no prior knowledge of their position and thus a localization mechanism is often a requirement. The process of localizing a 'blind' device consists of ranging estimates or angle measurements to a set of references with a prior knowledge of their position relative to a co-ordinate system and the position computation of the blind device in relation to the fixed references. This research focuses on the process of ranging to enable two-dimensional localization of sensing nodes within WSNs. Alternative ranging methods for the specified application field have not demonstrated their ability to meet the resolution and accuracy (resolution 0.3 m with accuracy better than ± 1.0 m line-of-sight) required. A novel radio frequency (RF) time-of-flight (TOF) ranging system is presented in this work to mitigate those problems. The system has been prototyped using a TI CC2431 development platform with ranging and data packet transfer performed on a single channel in the 2.4 GHz ISM frequency band. The frequency difference between the two transceivers involved with ranging is used to obtain sub-clock TOF phase offset measurement in order to achieve high resolution TOF measurements. Performance results have been obtained for the line-of-sight (LOS), non-line-of-sight (NLOS) and indoor conditions. Accuracy is typically better than 7.0m RMS for the LOS condition over 250.0m and 15.8m RMS for the NLOS condition over 120.0m using a sample average of one-hundred two-way ranging transactions. Indoors accuracy is measured to 1.7m RMS using a 1000 sample average over 8.0m. Corresponding results are also presented for the algorithms suitability for localizing sensor nodes in two-dimensions. Ranging performance is bound by the signal-to-noise ratio (SNR), signal bandwidth, synchronization and frequency difference between devices. This ranging algorithm demonstrates a novel method where resolution and accuracy are improved time dependent in comparison to frequency dependent methods using narrow-band RF.

Contents

Declaration of Authorship xi

Acknowledgements xiii

Nomenclature xiv

1 Introduction 1
- 1.1 Overview of Sensor Networks . . . 1
- 1.2 Research Justification . . . 3
- 1.3 Research Aims . . . 6
- 1.4 Research Contributions . . . 8
- 1.5 Research Questions . . . 9
- 1.6 Research Methodology . . . 10
- 1.7 Thesis Structure . . . 11

2 Wireless Sensor Networks and Ranging 13
- 2.1 Individual Wireless Sensor Nodes . . . 13
  - 2.1.1 Architecture . . . 14
  - 2.1.2 Application Hardware . . . 15
  - 2.1.3 Power Considerations . . . 16
- 2.2 Wireless Communication and Networking . . . 18
  - 2.2.1 The Protocol Stack . . . 19
  - 2.2.2 Communication Protocol . . . 23
- 2.3 Ranging in WSNs . . . 25
- 2.4 Discussion . . . 38

3 Limitations of Ranging 43
- 3.1 Measurement Resolution . . . 43
- 3.2 Measurement Accuracy . . . 46
- 3.3 Synchronization . . . 51
- 3.4 Wireless Channel Effects . . . 54
- 3.5 Discussion . . . 59

4 Prototype Ranging System 61
- 4.1 Ranging Algorithm . . . 62
- 4.2 System Implementation . . . 69
  - 4.2.1 Prototyping platform . . . 69
  - 4.2.2 Frame format and timing extraction . . . 70

4.2.3 Software algorithms . . . 72
4.2.4 Interference issues . . . 75
4.2.5 Error margin . . . 76
4.3 Discussion and Summary . . . 80
4.4 Results . . . 81

5 Prototype Locating System **91**
5.1 Summary of Locating Systems and key parameters . . . 92
5.2 Position Estimation Problem . . . 93
5.3 System Implementation . . . 96
5.3.1 Position Estimation Algorithm . . . 96
5.3.2 System Description . . . 98
5.3.3 Software Overview . . . 100
5.4 Results . . . 103
5.5 Summary . . . 110

6 Results Analysis **111**
6.0.1 Resolution and Synchronization . . . 112
6.0.2 Noise Performance . . . 117
6.0.3 Multipath and Shadowing Effects . . . 119

7 Conclusions **123**
7.1 Summary of Work . . . 123
7.2 Suggested Further Work . . . 125

A Publications **129**

Glossary **145**

Bibliography **152**

List of Figures

1.1 Basic block structure of a wireless sensor node. 2
1.2 An example of a wireless sensor node for environmental monitoring. . . . 3
1.3 Tracking performance of Ubisense UWB locating system. 6

2.1 A general model of a wireless smart sensor. 15
2.2 Examples of wireless sensing nodes. 16
2.3 OSI and Zigbee stack reference models. 20
2.4 Wireless network communication and data routing topologies. 22
2.5 IEEE 802.15.4 standard data frame format. 26
2.6 Time and frequency domain response illustration. 27
2.7 Timing diagram of synchronized TOF ranging. 28
2.8 Time-difference-of-arrival architectures. 31
2.9 Timing diagrams for time-difference-of-arrival architectures. 31
2.10 Received signal strength fading components. 33
2.11 Characteristic of NFER phase and wavelength with range. 36
2.12 Triangulation in AOA localization. 38

3.1 Time diagram of TOF sub-clock period phase measurement. 45
3.2 Cramer-Rao lower bound estimates for TOF ranging. 48
3.3 Two-way time transfer technique for TOF device synchronization. 52
3.4 Wireless channel multipath and shadowing examples. 54
3.5 Canonical power delay profile representation for multipath signal arrivals. 57

4.1 Timing diagram illustrating resolution limitation for synchronized TOF ranging. 63
4.2 Vernier delay line schematic diagram. 63
4.3 Vernier delay line principle using different frequency inputs. 64
4.4 First timing diagram for Vernier delay line principle. 65
4.5 Second timing diagram for Vernier delay line principle. 65
4.6 Timing diagram of two-way time-of-flight ranging with sub-clock phase offset measurement. 67
4.7 Block diagram of TI CC2430 radio module. 70
4.8 Modulator and Demodulator block diagrams. 71
4.9 Frame perspective time diagram for two-way TOF ranging 72
4.10 Schematic illustration of IEEE 802.15.4 Compliant Ranging Frame. 73
4.11 Software flow diagrams for two-way ranging. 74
4.12 Signal correlator drift capture for TI CC2420. 77
4.13 Two-way ranging with sub-clock phase offset measurement using the TI CC2430. 77

4.14 Illustration of auto-correlation output function. 78
4.15 Signal correlation error correction method. 80
4.16 Performance of the ranging algorithm for the LOS condition. Ranging estimate versus GPS measured distance. 83
4.17 Performance of the ranging algorithm for the LOS condition. GPS measured distance versus time. 83
4.18 Photo showing LOS testing location. 84
4.19 Photo showing NLOS test location. 84
4.20 Performance of the ranging algorithm for NLOS condition. Ranging estimate versus GPS measured distance. 86
4.21 Performance of the ranging algorithm for the NLOS condition. Ranging estimate and GPS measured distance versus time. 86
4.22 Photographs of residential flat hallway and living room used for indoor ranging experiments. 87
4.23 Scale diagram of the residential flat used for indoor testing of the ranging algorithm. 87
4.24 Performance of the ranging algorithm for the indoor condition. Ranging estimate versus measured distance. 88
4.25 Real-time motion performance of the ranging algorithm for indoor condition. Ranging estimate versus measured distance. 88
4.26 Histogram count of round-trip timed values for 5000 two-way TOA measurements. 89

5.1 Position estimation of a blind device in two-dimensions by the intersection of ranging rings. 95
5.2 Resolving position ambiguity by required plus additional range measurements. 96
5.3 Simulated position estimation with effects of dilution of precision. 97
5.4 Block diagram of prototype locating system architecture. 99
5.5 Screen shot of locating system graphical user display. 103
5.6 Position estimation performance of locating system for outdoor LOS condition. 105
5.7 Histogram of collected x co-ordinate data for outdoor LOS condition. . . . 105
5.8 Position estimation performance of locating system for indoor NLOS condition. 106
5.9 Histogram of collected x co-ordinate data for indoor NLOS condition. . . 106
5.10 Outdoor real-time position estimates using Python software algorithm. . . 108
5.11 Indoor real-time position estimates using Python software algorithm. . . . 109

6.1 Effect of averaging on ranging performance for the LOS condition. 113
6.2 Non-linear characteristic of TOF ranging. 113
6.3 Distribution round-trip time estimates for outdoor LOS condition for different initiator-responder separation distances. 114
6.4 Model of TOF phase measurement techniques for ideal and non-ideal cases. 114
6.5 Effect of error in sub-clock phase measurement. 116
6.6 Ranging performance for different frequency offsets. 118
6.7 Filtering algorithm for ranging. 120
6.8 Real-time performance of ranging algorithm with filtering. 121

List of Tables

1.1 Predicted accuracies for GPS Standard positioning and precise positioning services. . . . 5
1.2 Ranging specifications for wireless sensor networks. . . . 7

2.1 Hardware specifications for Crossbow MICAz MPR2400CA and Texas Instruments TI CC2430 sensor nodes. . . . 17
2.2 Reported path loss exponent values for different environments. . . . 33

4.1 Relationships between parameters for TOF ranging system with phase offset measurement. . . . 64
4.2 Expected lower bound variance for a single range estimates using IEEE 802.15.4 with different preamble sequence duration. . . . 72
4.3 Prototype ranging system estimation errors measured relative to the GPS range estimate. . . . 89

5.1 Key parameters of available locating systems. . . . 94
5.2 Locating system cumulative fraction of readings with error less than abscissa, 200 position estimates for outdoor LOS and Indoor NLOS conditions. 107
5.3 Z-locating engine RSSI locating results for Outdoor LOS and Indoor NLOS conditions. . . . 107

Declaration of Authorship

I, Bjorn Thorbjornsen, declare that the thesis entitled Radio Frequency Ranging for Wireless Sensor Network Localization, and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as: Radio frequency (RF) time-of-flight ranging for wireless sensor networks; A Local Positioning System (LPS) using RF Time of Flight Ranging.

Signed: Bjorn Thorbjornsen

Date: 03 November 2010

Acknowledgements

I would especially like to thank Professor Neil White, Professor Andrew Brown and Dr Jeff Reeve for their supervision, support and guidance throughout my PhD. I would also like to express my appreciation to Dr Nick Harris for providing excellent feedback for both my nine-month and eighteen month progress reports during my PhD. In addition to the help and support provided by the aforementioned, I would also like to thank Richard Seely for his effort in helping to carry out on the field testing and experimentation that have obtained some of the results herein. I also express my sincere appreciation to the School of Electronics and Computer Science, University of Southampton for supporting me by means of a doctoral training award and providing excellent research facilities during my time of study.

On a final note, I wish to also thank the Electronic Systems and Device (ESD) research group, especially Evangelos Mazomenos for the constructive discussions and suggestions which have helped me produce this thesis. I would also like to thank Dr Geoff Merrett for organising the WiSE meetings and online website enabling research to be shared between all parties.

Nomenclature

A	Amplitude
Acc	Accuracy
b_i	The i^{th} time quantization bin
B	Bandwidth
c	Speed of light
c_{aco}	Speed of an accoustic signal
ck	System clock
$C(\epsilon xyz)$	Minimum cost
d	True distance
d_i	range-sum
D_s	Doppler spread
d_0	Zero-reference distance
$\hat{d}$	Estimated distance
E	Modulus of elasticity
E_b	Energy per bit
E_s	Signal energy
F_s	Sampling frequency
f_0	Carrier frequency
G_r	Receiver antenna power gain
G_t	Transmitter antenna power gain
$H(f)$	Frequency Response function
$\angle H(f)$	Frequency Response phase offset
k	Boltzmann constant
N	Sample number
N_0	Noise power
$\hat{P}_{ei}$	Estimated range sum
P_i	Pseudorange estimate to the i^{th} point
P_o	Average noise power
P_r	Receive power
P_s	Average signal power
P_t	Transmit power
$\hat{P}_r$	Measured received power

r	Bit rate
R	Resolution
Ref_i	The i^{th} reference device
R_x	Receiver
$s(t)$	Input signal
t_{ck}	Transmitter-receiver relative clock offset
T	Temperature
t_b	Time period of responder system clock cycle
t_{clk_in}	Input clock period
t_d	Sub-clock phase offset
T_{delay}	Time difference in propagation delay
t_{direct}	Direct signal propagation delay
t_{iR}	Reception time at the i^{th} device
t_{iT}	Transmission time at the i^{th} device
$t_{i-transmit}$	Transmit time at the i^{th} device
$t_{j-offset}$	Phase offset of the j^{th} device clock relative to the system reference clock
$t_{reflect}$	Reflected signal propagation delay
$t_{ref-clk}$	Reference clock period
T_s	Sampling period
t_{sync}	Synchronization period
T_{tof_off}	Time-of-flight sub-clock time period
T_x	Transmitter
$t_{(i\rightarrow j)}$	Measured time at the j^{th} clock relative to the i^{th} device clock
t_{iRES}	Response delay period at the $i^{th}device$
t_ϕ	Phase offset position
v	Velocity
$X(f)$	Input signal
$x(t)$	Complex signal envelope
X_σ	Random noise contribution
$Y(f)$	Output signal
(u, v)	Position estimate
(x_i, y_i)	Position of the $i^{th}point$
α_0	Received signal amplitude
α_n	Received amplitudes of multipath returns
$\tilde{\alpha}_n$	Multipath-to-direct signal ratio
β	Propagation factor
γ	Path loss exponent
Δd	Change in distance
Δs	Change in displacement
Δt	Change in time / time difference
Δt_i	Relative phase offset of the i^{th} device

Δv	Change in velocity
Δ_Φ	Phase angle
ϵ	Permittivity
ϵ_i	Error in the i^{th} range estimate
ϵ_{xyz}	Position estimate error
ζ	Ratio of the molar heat capacities of the gas
η	Unitless constant, combined measure of d_0 and γ
θ_i	Angle of the i^{th} point
λ	Signal wavelength
μ	Permeability
ρ	Density of the medium
σ_{TOA}	Time-of-flight measurement variance
$\sigma_{\epsilon(i)}$	The i^{th} error variance component
τ	Time offset
τ_n	Propagation delay of multipath signal path
$\tilde{\tau}_n$	Excess delay of multipath returns
Φ	Power flux density
ϕ_n	Receiver carrier phase of multipath return

List of Abbreviations

ADC ..... Analogue-to-Digital Converter
AFE ..... Analogue Front End
AM ..... Amplitude Modulation
AOA ..... Angle of Arrival
API ..... Application Program Interface
ATR ..... Acceptance To Range
AWGN ..... Additive White Gaussian Noise
BPSK ..... Binary Phase Shift Keying
CDF ..... Cumulative Distribution Function
CEP ..... Circular Error Probable
CRB ..... Cramer-Rao Bound
CSR ..... Cambridge Silicon Radio
DAC ..... Digital-to-Analogue Converter
DOP ..... Dilution of Precision
DPM ..... Dynamic Power Management
DSO ..... Digital Storage Oscilloscope
DSP ..... Digital Signal Processor
DSSS ..... Direct Sequence Spread Spectrum
EEPROM ..... Electrically Erasable Programmable Read-Only Memory
EPROM ..... Erasable Programmable Read-Only Memory
FCC ..... Federal Communications Commission
FCS ..... Frame Check Sequence
FFD ..... Full-Function Device
FHSS ..... Frequency Hopping Spread Spectrum
FIFO ..... First In First Out
FPGA ..... Field Programmable Gate Array
GFSK ..... Gaussian Frequency Shift Keying
GPS ..... Global Positioning System
HDOP ..... Horizontal Dilution of Precision
IC ..... Integrated Circuit
IEEE ..... Institute of Electrical and Electronics Engineers
ISM ..... Industrial, Scientific and Medical

ITU-R	International Telecommunications Union Radio communication Sector
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LNA	Low Noise Amplifier
LOS	Line of Sight
LPS	Local Positioning System
LQI	Link Quality Indication
LR-WPAN	Low-Rate Wireless Personal Area Network
LSB	Least Significant Bit
MAC	Medium Access Control
MAP	Maximum a Posteriori
MDR	Multipath to Direct Ratio
MDU	Microcontroller unit
MEMS	Micro-Electromechanical System
MFR	MAC Footer
MHR	MAC Header
MPDU	MAC Protocol Data Unit
MRSK	Multiple Frequency Shift Keying
MSB	Most Significant Bit
NFER	Near Field Electromagnetic Ranging
NIST	National Institute of Standards and Technology
NLOS	Non Line of Sight
O-QPSK	Offset-Quadrature Phase Shift Keying
OSI/RM	Open System Interconnection Reference Model
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
PDOP	Position Dilution of Precision
PDP	Power Delay Profile
PHY	Physical
POR	Power on Reset
PPM	Parts Per Million
PPS	Precise Positioning Service
PSD	Power Spectral Density
PSDU	PHY Service Data Unit
QoS	Quality of service
RAM	Random Access Memory
RF	Radio Frequency
RFD	Reduced-Function Device

RFID ..... Radio-Frequency Identification
RMS ..... Root Mean Square
RSS ..... Received Signal Strength
RSSI ..... Received Signal Strength Indication
RTR ..... Request To Range
SFD ..... Start of Frame Delimiter
SHR ..... Synchronisation Header
SNR ..... Signal-to-Noise Ratio
SoC ..... System-on-Chip
SPI ..... Serial Peripheral Interface
SPS ..... Standard Positioning Service
SRAM ..... Static Random Access Memory
SS ..... Spread Spectrum
TDMA ..... Time Division Multiple Access
TDOA ..... Time Difference of Arrival
TOA ..... Time of Arrival
TOF ..... Time of Flight
TWTT ..... Two Way Time Transfer
UART ..... Universal Asynchronous Receiver/Transmitter
USART ..... Universal Synchronous/Asynchronous Receiver/Transmitter
UWB ..... Ultrawide-band
VDL ..... Vernier Delay Line
VDOP ..... Vertical Dilution of Precision
WINS ..... Wireless Integrated Network Sensors
WLAN ..... Wireless Local Area Network
WPAN ..... Wireless Personal Area Network
WSN ..... Wireless Sensor Network

Chapter 1

Introduction

Ubiquitous computing was the name given by Mark Weiser in 1988 to describe computing of the 21st century, the third wave in computing proceeding the original mainframes and further advanced personal computers [1, 2, 3, 4]. The underlying idea of Ubiquitous computing is the integration of information processing into everyday objects and activities. Thus, Ubiquitous computing is also referred to as 'pervasive computing', 'ambient intelligence' or 'everywhere' [5, 6] indicating this integration of information processing. The ubiquitous computer user may engage with many computational devices simultaneously while using everyday objects such as kettles, coffee makers or mobile personal digital assistants (PDAs) without necessarily being aware of this. The vision of ubiquitous computers are that off small, inexpensive, hardware-constrained processing devices, distributed at all scales throughout everyday life which are application specific. On a personal scale, mobile phones, digital audio players, radio-frequency identification (RFID) tags and the global positioning system (GPS) are all examples of ubiquitous computers. Domestic and commercial control and monitoring systems including security, environmental climate control and lighting systems are all larger scale examples. There are a wide range of research fields involving the use of ubiquitous computing including mobile computing, human-computer interaction, artificial intelligence and RFID. The fundamental area or interest underlying all of those applications are wireless sensor networks (WSNs) [7].

1.1 Overview of Sensor Networks

"Wireless sensor networks could advance many scientific pursuits while providing a vehicle for enhancing various forms of productivity, including manufacturing, agriculture, construction, and transportation."

David Culler, University of California, Berkeley [8].

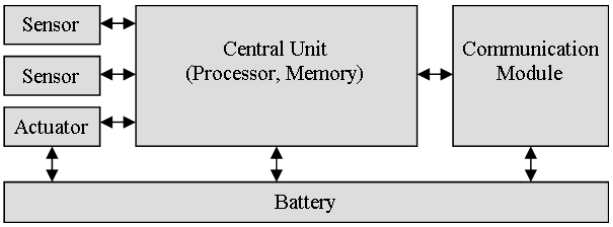


FIGURE 1.1: Basic block structure of a wireless sensor node (reproduced from Blumenthal *et al.* [7]).

Each year, computing capabilities become exponentially smaller and less expensive. Miniaturisation of semiconductor technologies has lead to the development of small, low-power and inexpensive sensor devices, often referred to as 'nodes'. Sensor nodes combine the abilities of computation, communication and sense in order to cooperatively monitor and control physical or environmental conditions at diverse locations. These individual devices within a WSN are inherently resource constrained: they have limited processing speed, storage capacity and communication bandwidth. However, in the aggregate, these devices have substantial processing capability and thus their many vantage points on the physical phenomena must be combined within the network itself [8]. Sensor nodes were originally envisioned to be low cost with the basic structure illustrated in figure 1.1. Each device is equipt with one or more transducers (sensors) and or actuators, a central unit consisting of microcontroller or microprocessor and memory module, radio transceiver for communication, and energy source (often a battery with the addition of an energy harvesting device). The size, weight and portability of those sensor nodes is fundamentally dependent on the physical size of the sensors, actuators and energy source involved. Sensor nodes can therefore range in size from millimetres to cubic metres. Sensor nodes can also be equipt with multiple sensors or actuators in order to measure a range of physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants. During operation, those sensor nodes detect events being monitored. Each event is processed by the sensor node and communicated to a centralized node using a single-hop or multi-hop communications protocol. The centralized node or 'base' then executes a specific operation based on an application specific algorithm. The development of WSNs are influenced by many factors because of their suitability for a wide range of monitoring, control and tracking applications. Physical size, power consumption and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational capability and bandwidth. In most WSN applications, sensor nodes must operate wirelessly for long periods of time, therefore the availability of energy typically limit their overall operational period. For this reason, energy consumption is reduced by switching off peripheral hardware systems on the sensor node for large periods of the operational duty cycle. In addition, sensor nodes may also incorporate energy harvesting or 'energy scavenging' devices such as solar panels or vibration energy harvesting devices to improve the operating life expectancy of the wireless network.

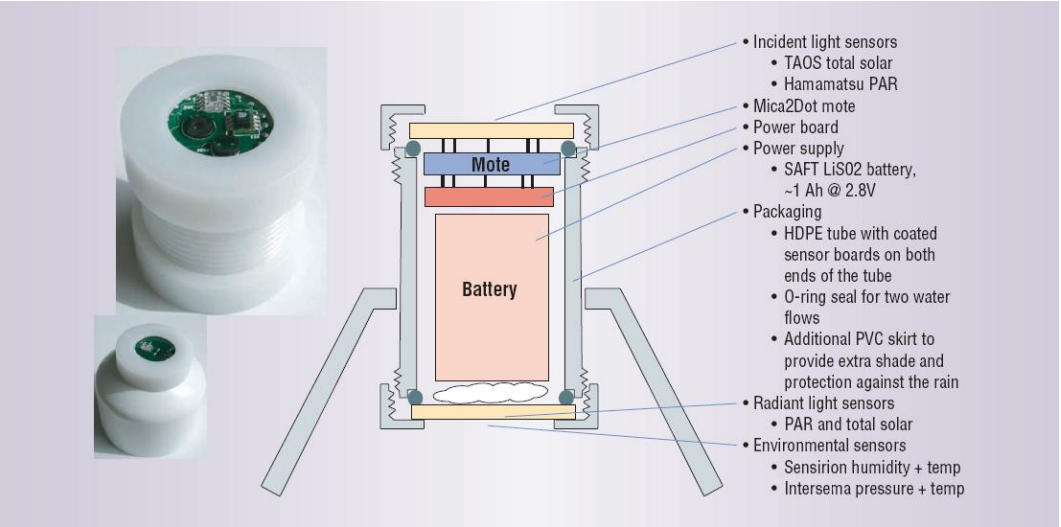


FIGURE 1.2: Example of a wireless sensor node for environmental monitoring. An entire wireless micro weather station fits in a tube approximately the size of a film canister [8].

WSNs hold promise for a wide range of monitoring, control and tracking applications in areas of hard accessibility or when wired infrastructure is not a feasible option. The application fields are however limited by processor performance, transmission range, radio sensitivity, power consumption, weight and size. A large number of WSN applications exist in but are not limited to domestic, commercial, industrial and medical systems. Figure 1.2 illustrates a typical example of a wireless sensor node. In addition, some well known research activities in the field of sensor networks are wireless integrated network sensors (WINS) [9], Smart Dust [10] and Sensor Webs [11]. There are also a number of more specific applications of WSNs in habitat monitoring [12], asset tracking [13], fire detection [14], traffic monitoring [15] and military tracking and surveillance [16]. At the time of writing, few commercialized WSN technologies were available and their main applications still remained in research projects.

1.2 Research Justification

There are a diverse range of WSN applications where wireless sensing nodes are often deployed without a prior knowledge of their position as illustrated in the previous section. The focus of this work is on ranging and basic localization in one class of wireless sensing applications. Those include domestic, environmental, commercial, industrial and medical systems where the sensor nodes in question are of low cost, standard with respect to hardware architecture and processing abilities and communicate using the low-power narrow-band radios (detailed in the next chapter) which are most commonly employed. Some examples of this class include but are not limited to an asset or personnel locating or tracking system for a commercial premises, large scale wireless climate control system

or an environmental or habitat monitoring system for large scale deployment (i.e. over an area of $1km^2$). In those applications, sensor nodes are typically in the order of 0.1 - 1.0 m in physical size. Based on the class of applications defined, a suitable ranging method to enable the localization process within those applications must have a resolution of 0.3 m or better and an accuracy of $\pm$1.0 m or better. This is because given the diverse range of propagation environments within this class of applications (i.e. LOS, NLOS and attenuated path), the physical size of sensor nodes and the metric of interest (i.e. a person's movement or assets location within an environment of interest), those constraints fit well and have been the goal within the field of research [17].

There are three key reasons why the ability to estimate the positions of sensor nodes is vitally important. Firstly, the location of sensing devices may continually change and a localization mechanism is required to estimate the positions to those individual sensors to make use of the data recorded by the sensor(s) on each device. Secondly, the measurement obtained by sensor nodes is only useful if corresponding location information is available. Thirdly, power consumption in WSNs is a primary concern. Efficient data routing is required to reduce power consumption and maintain the life expectancy of the WSN. Efficient routing of data requires knowledge of transmission distances between those sensor nodes. The process of determining the location of sensor nodes is known as localization and consists of two stages: 1) measuring the distance or angle between the sensor nodes; 2) computing position estimates of those sensor nodes based on the distance or angle measurements. When the process of localization is repeated over time, the sensor nodes can also be tracked. There has been a significant amount of research on position estimation algorithms for sensor localization, however, the ranging or angle measurement techniques on which they rely have not demonstrated the ability to meet the resolution and accuracy required for WSN localization (resolution 0.3 m with accuracy better than $\pm$ 1.0 m LOS). Estimating distance reliably to this level of resolution and accuracy within the constraints of sensor nodes including low power consumption, simplicity and low hardware overheads still remains a challenging task. Most applications of navigation, remote monitoring and PDAs utilise the Global Positioning System (GPS) which is the most predominantly used system for position, velocity and timing information. GPS provides continuous three-dimensional position and velocity information world-wide to users with the appropriate receiving equipment. The system consists of a constellation of nominally 24 satellites which are controlled and monitored from a world-wide ground network and is available to an unlimited number of users [18]. Table 1.1 summarises the predicted accuracies for the GPS standard positioning service (SPS) and GPS precise positioning service (PPS). A GPS receiver must receive direct path signals from at least four satellites to estimate position. This limits the operation of GPS to outdoor applications because the signal strength of GPS signals are too low to penetrate buildings. A typical GPS receiver is similar in size to a sensor node (i.e. GPS XE1610-OEMPVT receiver and TI-CC2430 development board) and have similar power consumption in full power mode (typically 20mA - 25mA @ 3.3 V) [19, 20].

TABLE 1.1: Predicted accuracies for GPS Standard positioning and precise positioning services [18].

	Horizontal	Vertical	UTC time transfer	Velocity measurement
SPS	22.0m (95%)	27.7m (95%)	200ns (95%)	0.2m/s (95%)
PPS	13.0m (95%)	22.0m (95%)	40ns (95%)	-

However, GPS position estimates are not accurate to better than ±1.0 m, the accuracy requirement of WSN localization. In addition, GPS does not operate well in urban canyons, indoor environments, areas of dense foliage and in non-line-of-sight (NLOS) conditions [17, 13]. Equipping sensor nodes with GPS capabilities is therefore considered an impractical approach for WSN localization and therefore a technique which is integral with the sensor node is required. Local positioning systems (LPSs) based on the use of Ultra-wideband (UWB) radio technology are also available. UWB-based LPSs are high performance with respect to their ability to provide precise position estimates (resolution of 0.3 m or better and accuracy better than ±1.0 m) of 'tagged' devices. The Ubisense and PAL650 UWB locating systems are examples of precise LPSs [21, 22].

PAL650: PAL650 is a commercialized UWB locating system by Multispectral solutions [23, 21]. The system utilises TDOA ranging system with cabled infrastructure to determine the location of transmit-only tags. UWBs positioning capabilities combined with its low power operation and short broadcast time make it ideal for asset tracking with very large numbers of tags. The PAL650 system operates indoors with range up to 90 m with accuracy ± 0.3 m [21]. Position estimation variance is reported better than ± 0.10 m and ± 0.50 m in the x-y axis using a David-Fletcher-Powell minimization algorithm to compute the position estimate in three-dimensions [21]. As with the Ubisense system, the wired connectivity between base stations in order to meet the synchronization requirements limits the applications of this technology to fixed architecture.

Ubisense: Ubisense operates using UWB to locate a set of transmitter tags which are attached to objects. Tag transmissions are detected by a set of networked base stations which have known positions within the area to be instrumented. Each base station is capable of determining both distance estimates and signal angle-of-arrival (AOA) transmitted from the tags. Figure 1.3 illustrates the measurement performance of the prototype Ubisense system. The accuracy is indicated by the distributed tag position estimates at each grid intersection. The translation of range error to the position estimate is illustrated by the differing magnification of error and is known as geometric dilution of precision (GDOP) which will be explained later [24].

The operating range of those systems is limited though regulation on the maximum allowable transmission power of UWB signals (signals with bandwidth >500 MHz).

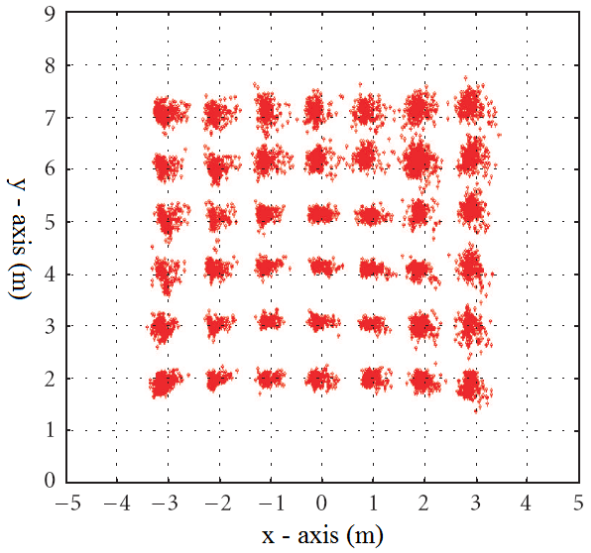


FIGURE 1.3: Tracking performance of Ubisense UWB locating system. Two base stations used to locate within a 10 metre square area. Single tag placed at one metre grid intersections over test area. 2003. [24]

Furthermore, wired infrustructure is a requirement between referencing architecture for timing synchronization. Those overheads limit the suitability of those systems for localization within WSN applications where low cost resource constrained hardware must operate wirelessly with low power consumption over long transmission ranges. Furthermore, precise localization ability is beyond the scope of wireless sensing applications as will be explained in the next section.

1.3 Research Aims

The performance of a distance estimation technique can be categorised by its resolution and accuracy. The measurement resolution R (m) defines the smallest change in distance Δd (m) that the system can detected. The accuracy Acc (m) defines the difference between the true distance d (m) and the estimated distance $\hat{d}$ (m) of the measurement ($Acc = (d - \hat{d})$). It is uncommon for a distance estimation system to *always* be accurate to within x metres because most distance estimation systems generate a small proportion of outlayers [24]. Therefore accuracy is commonly specified by the root-mean-square (RMS) error of the estimates or the accuracy level that 50% of the estimates will meet. A key problem is that the ranging and localization techniques current employed on sensor nodes do not meet the accuracy requirements of the diverse range of wireless sensing applications. For example, the Texas Instruments TI CC2431 (i.e. a typical sensor node platform) incorporates a received signal strength (RSS) based localization engine [20] with a specified resolution of 0.25 m and accuracy better than 3.0 m LOS. This level of localization accuracy would be unsuitable for an asset tracking system that must be

TABLE 1.2: Ranging specifications for wireless sensor networks.

Specification	Value	Condition
Resolution	0.3m	-
Accuracy	± 1.0m	Line-of-sight condition for 50% of estimates
	± 2.5m	Non-line-of-sight condition for 50% of estimates
Range	0.0m - 100.0m	Line-of-sight condition
	0.0m - 25.0m	Non-line-of-sight condition
Latency	< 0.1s	-

able to distinguish the positions of items with accuracy better than ± 2.5 m in separate rooms. RSS localization is also reported to have poor resilience to reflected signals (a common problem for indoor environments) and complex models are required to correct for errors [25]. In addition to the accuracy and resolution requirements, wireless sensing has a diverse range of applications that involve sparse or dense distribution and short or long range operation. An Asset tracking system may consist of 30 'tags' that must be tracked real-time (i.e. position estimate computation time less than 1 s) and operate indoors (NLOS conditions) over a range of 0.0 m - 25.0 m. In contrast, a habitat monitoring system may consist of over 100's of sensor nodes and operate outdoors (LOS conditions) over a range of 0.0 m - 100.0 m. For those reasons, a distance estimation method for use in wireless sensing applications should have the parameters for the resolution, accuracy, operating range and latency listed in table 1.2 which closely agree with [17, 26]. As a general note, when we refer to an *accurate* distance estimation in this work, we mean an estimate that meets the accuracies specified in table 1.2 for the said condition. Ranging systems that aim to have parameters beyond those in table 1.2 are referred to as *precise* ranging systems [23, 24] and are considered beyond the scope of wireless sensing applications. This is because sensor nodes are typically 0.1 m - 1.0 m in physical size and therefore this level of accuracy and resolution is not required in most cases. This work aims to research and develop a distance estimation technique that can meet the specifications in table 1.2 and operate within the constraints of WSNs including low power consumption, limited processing power and resource constrained hardware. This would enable the performance of localization required for the diverse range of wireless sensing applications. Thus, there are two fundamental parts to this work including estimating point-to-point distance, a process known as ranging and an algorithm to compute the position of the device in question once a set of range estimates have been obtained. The algorithms must be adaptable to standardized WSN hardware and protocols as defined by the class of application. Analysis and testing of the algorithms will be performed using commercially available off-the-shelf hardware to justify and validate the performance of the prototyped systems. Finally the performance of the algorithm will be evaluated and concluded for its suitability for wireless sensing applications.

The key areas of this research are summarized as follows:

Distance estimation system: Research and develop a distance estimation system that can meet the specifications summarised in table 1.2 and operate within the constraints of wireless sensor nodes. Those include low power operation, low complexity and low hardware overheads.

Position estimation: Research and develop a position estimation system to enable the two-dimensional localization of sensor nodes and verify the performance of a prototype ranging estimation system. The position of a sensor node with no prior knowledge of its position, often referred to as a 'blind' device will be computed in relation to a set of devices with knowledge of their positions, referred to as references and the position estimate will be displayed graphically in relation to the references. This system will be used to verify the developed ranging techniques suitability for the process of two-dimensional localization within WSNs. It is expected that the prototype and developed localization technique could be extended to enable three-dimensional localization ability, however, this is outside the scope of this research which is fundamentally based on ranging within the specified class of wireless sensing applications. The position estimation algorithm should be able to operate reliably in the presence of inaccurate ranging estimates and with real-time computation to enable its suitability for two-dimensional WSN-based locating and tracking applications.

1.4 Research Contributions

The following novel research contributions herein are summarized as follows:

Radio Frequency (RF) Time-of-Flight Ranging for Wireless Sensor Networks: A novel TOF-based ranging algorithm is presented to estimate point-to-point range between two sensor nodes involved with the localization process of a WSNs. The technique mitigates the use of large spectral bandwidth and frequency dependence in alternative RF-TOF ranging methods [17]. The algorithm can also meet the aforementioned constraints of WSNs and estimate range with the resolution and accuracy requirements of WSN localization. Frequency difference between two transceivers is used to measure sub-clock period phase offset measurements and thus, time-dependently determine pair-wise distance estimates with resolution and accuracy comparable to alternative frequency dependent TOF techniques using significantly higher timer clock frequencies [17, 26].

A Local Positioning System (LPS) using RF Time-of-Flight Ranging: A novel localization system has been developed to enable the position of a blind

sensor node within a WSN to be determined relative to a set of reference nodes using commercially available hardware. Two-way RF TOF ranging has been utilised for range estimation between blind devices and references where synchronization is relaxed and no wired connectivity exists between referencing architecture. The system has demonstrated its ability to enable the location of a blind sensor node to be determined to within ± 0.5 m for over 75% of position estimates for LOS conditions. To the best of the author's knowledge, this is the first narrow-band RF localization system to demonstrate this level of locating accuracy using narrow-band RF TOF ranging. The use of narrow-band RF signals also allow operational range within regulation over much greater distance (>100.0 m) than alternative UWB-based locating systems [13] and enables the localization accuracy requirements of WSNs.

Publications

- B Thorbjornsen and N M White and A D Brown and J S Reeve, Radio frequency (RF) time-of-flight ranging for wireless sensor networks, Measurement Science and Technology, vol. 21, no. 3, pages 035202, 2010.
- B. Thorbjornsen, R. Seely, N.M. White and J.S. Reeve. In press. A Local Positioning System (LPS) using RF Time of Flight Ranging. IEEE Sensors Journal.

1.5 Research Questions

- **What class of wireless sensing applications does this work focus on?** This research focuses on ranging and basic localization in domestic, environmental, commercial, industrial and medical systems where the sensor nodes in question are of low cost, standard with respect to hardware architecture and processing abilities and communicate using the low-power narrow-band radios which are most commonly employed. Examples of the class of application include asset or personnel locating or tracking system for a commercial premises, large scale wireless climate control system or an environmental or habitat monitoring system for large scale deployment (i.e. over an area of $1km^2$).
- **Why is localization important in wireless sensor networks?** On deployment, sensor nodes normally have no prior knowledge of their position; however, position information of sensor nodes within those WSNs is often a requirement to make use of the data recorded by the sensors themselves. Therefore, a localization mechanism is required to estimate their positions.
- **What is the process of localization?** Localization involves two stages: 1) distance estimates or angle measurements to a set of reference nodes which have a

prior knowledge of their position relative to a co-ordinate system; 2) the computation of the position of the blind device in relation to the set of references.

- **Why is a novel ranging method required for the defined class of WSN applications?** Alternative distance estimation methods have not demonstrated their ability to meet the resolution and accuracy requirements specified in table 1.2 under the constraints of the class of wireless sensing applications defined such as low complexity, low cost and low power operation.

- **What defines the accuracy of a ranging system?** The accuracy of a ranging system Acc (m) defines the difference between the true distance d (m) and the ranging systems estimated distance $\hat{d}$ (m) of the measurement ($Acc = (d - \hat{d})$). The accuracy is bound by a number of factors, those are detailed in chapter 3.

- **What defines the resolution of a ranging system?** The measurement resolution of a ranging system R (m) defines the smallest change in distance Δd (m) that the ranging system can detected. The resolution is bound by a number of factors, those are detailed in chapter 3.

1.6 Research Methodology

The research methodology of this work is summarized in the order it is presented as follows:

Wireless Sensor Networks and Ranging An overview of WSNs including their application, hardware overheads, processing abilities, key considerations, communication and networking protocol and the methods and techniques of ranging and localizing those wireless sensing devices. The chapter summarises the background field and motivation for the choice of RF TOF ranging as a feasible technique for ranging and localization within the defined field of WSN applications.

Limitations of Ranging Explores the limitations in performance of TOF ranging. There are four identified limitations including measurement resolution, measurement accuracy, synchronisation and the effects of the wireless propagation channel on TOF ranging. Those are explained in detail to provide the reader with an in depth knowledge of the performance limitations of TOF ranging. The chapter summarizes the limitations and highlights the key methods of mitigating those limitations to the best extent. The summary also emphasises why narrow-band RF TOF ranging is an good choice of ranging technique in the specified field of WSNs.

Prototype Ranging System This chapter builds on the development of a novel RF TOF ranging technique using the principle of the Vernier delay line digital

structure in order to improve the performance of the system beyond alternative frequency dependent ranging methods utilising RF TOF. The work addresses how the limitations in TOF ranging performance addressed in chapter 3 are overcome. It is identified that synchronization in TOF ranging is a key concern for error and details how the error contribution from this source can be reduced. The chapter provides clear timing diagrams of the technique in order to justify the function of the system and highlight the novel contribution. The prototyping platform, data packet frame format, timing extraction, software algorithms and error margins are explained in detail. Preliminary performance results are provided and the key conclusions of the chapter are summarized.

Prototype Locating System A two-dimensional localization system is developed in order to illustrate the performance of the ranging technique developed in chapter 4 for the purpose of localization in wireless sensing applications. The chapter summarizes the key constraints involved with the process of localization including position estimation techniques, geometry and dilution of precision of range estimates and system architecture. This chapter aims to justify that RF TOF ranging is a suitable technique for the localization process of WSNs. Results are presented for both LOS and NLOS conditions and the research is summarised.

Results Analysis This chapter focuses on the errors associated with the RF TOF ranging algorithm in further detail using simulation and results analysis. The work illustrates that the function of clock drift between two sensor nodes involved with the ranging process is a key function in order to improve the accuracy of ranging estimates. Noise performance and the effects of multipath and shadowing are summarised in further detail and it is shown that the implementation of a simple filtering algorithm can be used to reduce ranging errors associated with noise and multipath signal propagation.

Conclusions The work is summarized and concluded for both ranging and localization with suggested further work to improve the performance of the algorithms developed herein.

1.7 Thesis Structure

Chapter 2 provides an overview of sensor nodes, their constraints, hardware architecture and a summary of ranging techniques. The background research has been summarized and a conclusion is drawn that radio frequency time-of-flight (RF-TOF) ranging is a suitable technique for range estimation within WSNs. Chapter 3 details the limitations of TOF ranging from four perspectives including resolution, accuracy, synchronization requirements and the effects the wireless channel. A novel RF TOF ranging method is presented in chapter 4 with its suitability for operation on low power, low cost wireless

sensing hardware. The system has been implemented on a Texas Instruments CC2430 development kit. In chapter 5 a simple localization system is presented using the developed RF TOF ranging method which operates with relaxed clock synchronization and requires no wired infrastructure between referencing architecture for synchronization as with alternative locating systems utilising TOF ranging. Results and analysis of both systems are presented in chapter 6 where ranging and localization performance is demonstrated for both the outdoor LOS and indoor NLOS condition. A filtering algorithm is implemented to reduce error in range estimates. Conclusions and suggested further work is presented in chapter 7.

Chapter 2

Wireless Sensor Networks and Ranging

Wireless sensor networks combine the abilities of computation, communication and sense at remote locations to collectively monitor, control or track quantities of measurement within an area of interest. They hold promise for a wide range of applications in buildings, utilities, industry, homes, transportation, security and healthcare enabling the key to intelligently and efficiently gathering information and measurement using low cost and inexpensive resource constrained devices. Quantities can be sensed and measured in applications where the use of cabling is either uneconomic or an impractical solution. However, there are challenges including detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, making logical decisions and displaying the data in a meaningful format [27]. In this chapter an overview of WSNs is provided and the key challenges of both ranging and localization within those applications are presented. The technical aspects of ranging and localization within WSNs are discussed and concluded in order to select the method most suitable for adaption in compliant WSN hardware and communications protocol.

2.1 Individual Wireless Sensor Nodes

The ideal wireless sensor can be networked using a low-rate communications link, is scalable for sensing in large-scale applications, has low power consumption to maintain the life of the network, is smart and software programmable, capable of fast data acquisition, reliable and accurate over the long term, costs little to purchase and install and requires no real maintenance. The aim is to fit all mentioned features in a single chip solution [7]. Selecting the optimum sensors and wireless communications method require knowledge of both the application and the quantity(ies) of measurement required [28]. Thus, wireless sensors can be divided into categories where communication rate, sensor

update rate, life expectancy and physical size are all considerations for the design of the wireless sensor node. Some examples of low rate wireless sensors include temperature, humidity, pressure and strain. In contrast, examples of high rate sensors include acceleration, magnetic field, vibration and range estimation. The wide range of possible applications of sensor nodes means that their development has been influenced by many contributing factors. More recent advancements have resulted in the implementation of standardized sensing systems including the communications radio, microprocessor, memory and sensors on a single I.C. package. This enables a network of inexpensive sensor nodes with very low power consumption to communicate with each other using standardized hardware and systems including wireless communication protocols such as IEEE 802.15.4 [29]. The wireless network itself generally consists of a base station or 'gateway' that can communicate with a number of wireless sensors via the communication radio. Data is sensed at each wireless sensor node, compressed and transmitted to the gateway directly or if required, uses other sensor nodes to forward the data to the gateway. The transmitted data is then presented to the system through the gateway connection.

2.1.1 Architecture

The architecture of a sensor node involves the fundamental framework for the integration and communication of the many sensors and networks available on the market today. This removes the need for manufacturers to produce special transducers for every different sensor network application. The Institute of Electrical and Electronics Engineers (IEEE) and National Institute of Standards and Technology (NIST) have produced the IEEE 1451 specification which defines the integration and connectivity of smart sensor networks. A smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity [30]. Sensors may be added to the node as required. Sensor signal conditioning can be programmed as necessary or removed. The flash memory allows the remote nodes to acquire data on command from a base station, or by an event sensed by one or more inputs to the node. Furthermore, the embedded firmware can be upgraded through the wireless network in the field. The microprocessor or microcontroller has a number of key functions including managing the data collection from the sensors, performing power management functions, interfacing the sensor data to the physical radio layer and managing the radio network protocol.

The generalized model for a IEEE 1451 compatible smart sensor is shown in figure 2.1. The wide range of sensor node applications is addressed by the modular design approach. The key objectives of smart sensors include moving the intelligence closer to the point of measurement, making it cost effective to integrate and maintain distributed sensor systems, creating a confluence of transducers, control, computation, communication to-

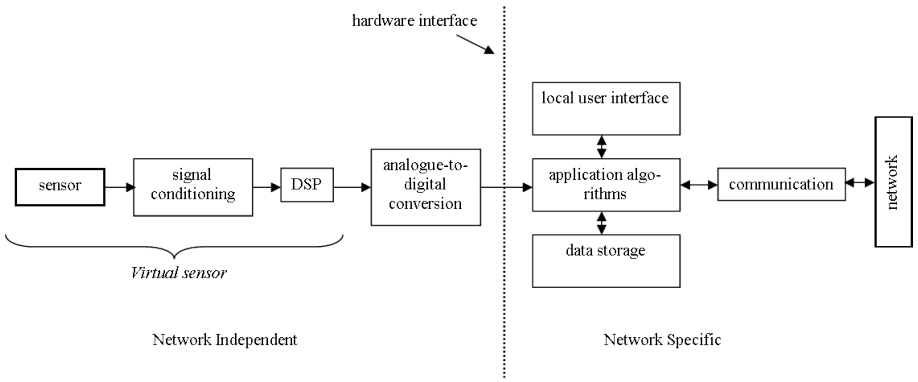
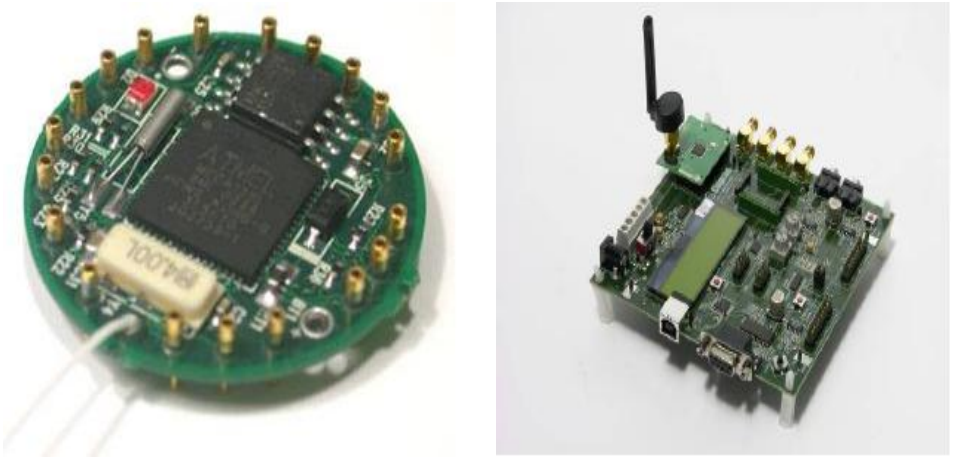


FIGURE 2.1: A general model of a smart sensor (IEEE 1451 Expo, Oct. 2001) [31].

wards a common goal and seamlessly interfacing numerous sensors of different types. IEEE 1451 specifies a communication architecture that is appropriate for WSNs, however, it does not specify the specifics about sensor interface [28]. IEEE 1451.1 aims to build on IEEE 1451 and standardize the communication interface of sensors to a wireless network. At the time of this research, IEEE 802.15.4 was the most widely accepted standard for the communication interface for sensor nodes within WSNs.

2.1.2 Application Hardware

There are a wide range of wireless sensor nodes available from companies including Crossbow, Cambridge Silicon Radio (CSR) , Lynx Technologies and Texas Instruments that are suitable for different wireless sensing applications. Two of the most widely accepted and diverse sensor nodes include Crossbow Berkeley motes and Texas Instruments TI CC2430DK development platforms. Those platforms provide a fast and effective prototyping solution for the development and test of most wireless sensing applications. Crossbow currently has a range of processor radio module families including MICA, MICAz, MICA2 and MICA2-DOT. Those sensing motes are mainly differentiated between by the radios baseband transmission frequency. Furthermore, all of those Crossbow sensor motes have a Atmel ATmega128L microcontroller and IEEE 802.15.4 Compliant RF transceiver. In contrast, the TI CC2431 development platform features the TI CC2430 I.C. which is a combined Intel 8051 microcontroller and IEEE 802.15.4 Compliant RF transceiver single chip solution for wireless sensing applications. Key parameters of both Crossbows MICAz (MPR2400CA) and the Texas Instruments CC2430 development platform are summarized in table 2.1. Those platforms have specifically been selected herein because they both operate in the 2400.0 MHz to 2483.5 MHz ISM frequency band and have similar capabilities. The main differentiation between those prototyping platforms is the number and type of standardized physical interfaces, the physical size and the energy source utilised. The maximum operating clock frequencies of the microcontrollers also differ significantly where the Crossbow MICAz are limited to 8 MHz and the TI CC2430 is limited to 32 MHz. The TI CC2430 therefore has a significant advantage



(a) Crossbow Berkeley MICA2-DOT (MPR500) sensing wirless mote [32].

(b) Texas Instruments SmartRF04EB with CC2431EM module wireless sensing node development platform [33].

FIGURE 2.2: Example of wireless sensing node platforms available for prototyping and developing WSN applications.

for applications that require high frequency timing such as TOA ranging which will be detailed in the proceeding sections.

2.1.3 Power Considerations

Power consumption is a primary concern for WSNs since sensor nodes may be distributed geographically in remote environments (i.e. sensors dropped from an aircraft for personal/vehicle surveillance) [27]. They are often expected to operate for long periods of time (> one month) from a single battery source which cannot economically be replace or recharged following deployment. For this reason alone, increasing the life expectancy of individual sensor nodes through the use of power conservation, power generation and power management systems is of great interest. In addition, the physical sizes of energy sources are a concern for some applications of WSNs. For example, a standard 3.0 V CR2450 lithium coin cell has energy density of 240 mAh/cm^3. A sensing device requiring 4 mAh per day with twelve month deployment would require 6.1 cm^3 of battery storage (4mAh/day x 365 days = 1460mAh, one coil cell holds 240mAh/cm^2, therefore total energy used/ energy per cell = 6.083 $\approx$ 6.1cm^2 of battery) [34].

The design of RF microelectromechanical system (MEMS) components including inductors and capacitors for RF transceivers and power generation MEMS using individual or combined solar, vibration (electromagnetic and electrostatic) and thermal technologies are some of the solutions for power management and conservation in WSNs [27]. In

TABLE 2.1: Hardware specifications for Crossbow MICAz MPR2400CA and Texas Instruments TI CC2430 sensor nodes.

	Crossbow MICAz (MPR2400CA)	TI CC2430DK (Smart RF04EB with CC2431EM module)
Processor		
General note	Atmel ATmega128L microcontroller	Intel 8051 microcontroller
Program flash memory	128k bytes	128k bytes
Measurement memory	512k bytes	4k bytes
Configuration memory	4k bytes (EEPROM)	8k bytes (4kB with data retention in all power modes)
Serial communication	UART	USART
Other interfaces	Digital I/O, 12C, SPI	Digital I/O, SPI
Current consumption	8mA (Active mode) <15uA (Sleep mode)	7mA (Active mode) 0.6uA (No clock, RAM retention, POR)
System clock frequency	8MHz (Crystal oscillator) 32kHz (External clock source)	32MHz (Crystal oscillator) 16MHz (Crystal/RC oscillator) 32.753kHz (low power RC oscillator)
RF Transceiver		
General note	IEEE 802.15.4 Compliant RF transceiver	IEEE 802.15.4 Compliant RF transceiver
Frequency band	2400.0MHz to 2483.5MHz	2400.0MHz to 2483.5MHz
Transmit (Tx) data rate	250kbps	250kbps
Number of channels	16	16
RF power	-24dBm to 0dBm	-25.2dBm to 0.6dBm
Receiver sensitivity	-90dBm(min), -94dBm(typical)	-94dBm(typical)
Outdoor range	75.0m - 100.0m	100.0m - 250.0m (typical as tested)
Indoor range	20.0m - 30.0m	15.0m - 45.0m (typical as tested)
Current consumption	19.7mA (Receive mode) 11mA (Tx, -10dBm) 17.4mA (Tx, 0dBm) 20uA (Idle mode, voltage regulator on) 1uA (Sleep mode, voltage regulator off)	27mA (Receive mode) 20.1mA (Tx, -10.8dBm) 24.7mA (Tx, 0dBm) 296uA (Power mode 1, 32.768kHz clock, RAM retention) 0.6uA (No clock, RAM retention, POR)
Electromechanical		
Energy source	2x AA batteries	1x PP3 battery
External power	2.7V - 3.3V	2.0V - 3.6V
Size (mm)	58 x 32 x 7	145 x 132 x 35
Weight (grams)	18	118
Connectors	51-pin expansion connector	2x 20-pin I/O ports
User interface	3 LEDs	Push buttons, potentiometer, joystick, 3 LEDs, LCD panel, audio filter and amplifier.
Software		
Operating system	Tiny-OS	Zibgee stack
Source code language	Nested-C (similar to C)	C/Assembler

addition to the development of hardware systems, software algorithms such as time division multiple access (TDMA) allow sensor nodes to power down or 'sleep' between its assigned time slots. This is effectively a power management system enabling the sensor node to wake up in time to receive and transmit messages. It is reported that low-power task scheduling operating systems are best suited for the requirements of sensor nodes [7]. This is because a task scheduling algorithm enables functions within the sensor node to be performed at the optimum time, for example, when battery power is high data is transmitted else the sensor node waits. The control of sensor node hardware by efficient software algorithms include but are not limited to event-driven sensor sampling and minimized sensor sampling rates for energy conservation. Microcontroller hardware used for sensor nodes provide a range of power saving techniques including dynamic power management (DPM) which switches off hardware components that are not required and uses clock scaling [7]. Both Crossbow sensor motes and the Texas Instruments CC2430 have those features available. Furthermore, they are both low power platforms that have

been developed for wireless sensing applications due to their low-rate radio modules, sleep operating modes, physical size and power consumption. The life expectancy of those sensing nodes is to an extent dependent on the software algorithms implemented on them where the developer must ensure they operate in a power efficient manner.

The most promising layers for energy savings are the physical, link and network layers [7] which are concerned with networking, transmission and reception of data. A wide range of strategies have been investigated and employed to reduce this overhead including data compression and reduction, reduced frequency of data transmission (transceiver duty cycle), event-driven transmission strategies and efficient data routing algorithms. For example, the transmission power required to transfer data between a source and destination increases by the square of the distance. Therefore, multiple short message transmission hops require less power than one long hop [27]. This is illustrated by considering the distance d between a source-destination and the transmission power proportional to d^2 that is required for transmission from the source to the destination. Using a multi-hop communication with n hops between the source and destination, the power required by each node is proportional to d^2/n^2. This suggests that distributed multi-hop network algorithms have the ability to reduce the power consumption of data communication and transfer in WSN applications.

2.2 Wireless Communication and Networking

Sensor nodes require a mechanism of adaption to the dynamical system or application in order to cumulatively make use of the data recorded by the individual sensors themselves and form the WSN application. This is the function of the communication protocol stack which provides the structuring for the application, method of communication and networking ability of the wireless sensing devices. The design and implementation requirements of the protocol stack can be summarized into the following categories:

Self-organisation: Individual sensor nodes must have the ability to self-configure and perform application-specific task automatically.

Co-operative processing: The fusion and combined processing of data recorded by multiple sensor nodes enables more precise and accurate results.

Security: Sensed data must be secure from spoofing and interception in a dynamic range of environments.

Power considerations: Network algorithms and communication protocols must operate efficiently to maintain the life expectancy of both the individual sensor node and the WSN.

In this section the protocol stack and communications protocols available for wireless sensing applications are outlined. The implementation of ranging and localization is considered for both the protocol stack and the communications protocols.

2.2.1 The Protocol Stack

The protocol stack is a hierarchy of software layers which implement a networking protocol suite. One of the most widely accepted protocol stack architecture reference models is the open system interconnection reference model (OSI/RM) illustrated in figure 2.3. Each layer implements a function a specific function of the networking and communication task. The basic OSI/RM open standard reference model is widely adopted by developers of standardized compatible systems interfaces. Each layer is self-contained enabling different implementations of that layer to be utilised in application specific protocol stacks. The protocol stack that has been developed specifically for the purpose of wireless sensing is known as Zigbee [35, 36]. Zigbee is an open specification protocol stack developed jointly by Zigbee Alliance and IEEE 802.15.4 [29] working group to complement the low-rate wireless personal area network (LR-WPAN) standard. The high level protocol stack reference model is illustrated in figure 2.3. Zigbee aims to enable low-rate, cost-effective, power efficient, reliable wireless networking capability for monitoring, control and tracking systems based on an open global standard. The lower layers incorporate the IEEE 802.15.4 standard and Zigbee provides the higher layers of the stack. IEEE 802.15.4/Zigbee compliant devices are intended to comply with the constraints of WSNs and be scalable to enable broad commercial adaption within cost sensitive applications. System-on-Chip (SoC) silicon solutions for IEEE 802.15.4/Zigbee applications are therefore optimized to meet the challenges including energy efficiency, low-cost and low-rate communication [37]. The function of each layer in order of the Zigbee protocol stack is described below.

Application Layer: Provides the services which directly support an application running on the host. These services are directly accessible by an application via common well-known application program interfaces (APIs) , which can occur at many layers.

Application Interface Layer: Performs the necessary data transformations or formatting required between the application layer and the lower stack layers. Functions provided by the application interface layer include data compression, file formatting and encryption.

Network Layer: Defines the functions necessary to support data communication between directly or indirectly connected entities. It is responsible for the operation of the network including device discovery, packet control, packet congestion, network configuration and networking topologies. It also provides the capability

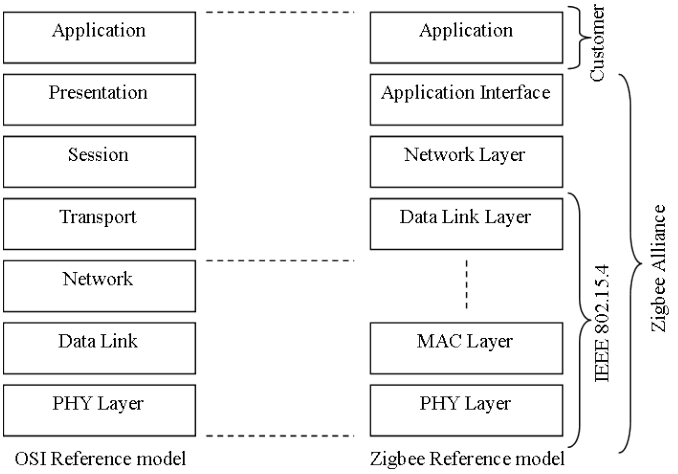


FIGURE 2.3: OSI and Zigbee stack reference models [28, 38].

of forwarding messages from the network layer entity to another until the final destination is reached. Wireless networking capabilities of operation in star, mesh and hybrid star-mesh topologies aim to standardize the protocol stack for a wide application field.

Data Link Layer: The data link layer accepts the unstructured bit stream provided by the PHY layer and provides reliable transfer of the data between two directly-connected data link layer entities. The data link layer functionality is limited in scope-delivery of messages over a local area. It is sub-divided into two sub-layers; medium access control and logic link control which more specifically define the primary aspects of data link layer functionality.

Medium Access Control (MAC) Layer: Provides access and control of the physical layer for all types of data transfer, Logic link control (data framing, flow and error checking/correction) and Medium Access Control (controlling multiple accesses to a shared communications medium).

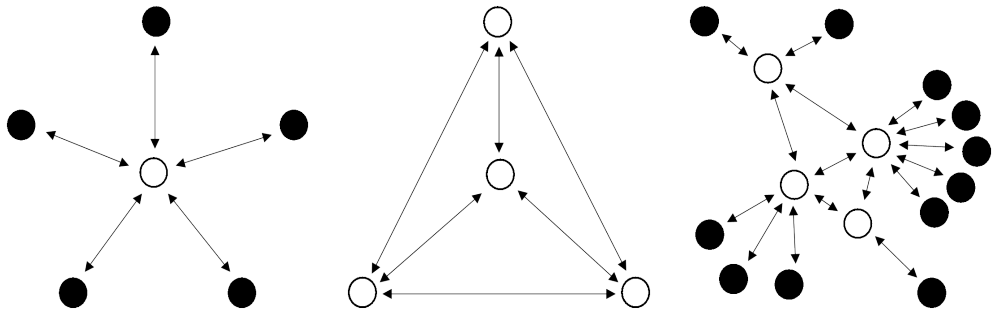
Physical Layer: Includes the device RF radio transceiver for communication to directly connected physical entities with low-level control mechanisms such as timing and communication control. Channel coding and modulation at bit-level are performed by the physical (PHY) layer which, can be used by higher layers to provide the basis for higher layer communication services. Physical properties include electromechanical characteristics of the medium or link between the communicating physical entities such as connectors, voltages and transmission frequencies.

Summarizing the layers of the Zigbee stack indicate that ranging is carried out in the PHY layer and the process of localization is implemented in the network layer. This is illustrated by the TI CC2431 which is compatible with the Zigbee protocol stack and incorporates a locating engine based on received signal strength indication (RSSI).

Thus, any ranging algorithm developed for compatibility with wireless sensing applications should also operate within the PHY and MAC software layers of the Zigbee protocol stack to reduce hardware overheads, power consumption and the complexity of individual sensing nodes. In addition, the ranging method must be scalable in order to enable large-scale WSNs. Furthermore, the method must be performed within a realistic time period, operate with low power consumption to prolong the life of the network and operate in conjunction with data transfer to reduce network traffic. In this work, the focus is on ranging and thus the PHY and MAC layers of the Zigbee stack. Since IEEE 802.15.4 PHY and MAC layers are incorporated in the Zigbee stack, this research is focused on ranging using this wireless standard. Consideration of the adaption of ranging in different Zigbee network topologies and routing algorithms is also important because they are linked. A prescribed network topology and routing algorithm are chosen to transfer packets from a source to a destination with an acceptable message throughput and quality of service (QoS) . Throughput is a measure of the percentage of packets that are successfully transferred from the source to the destination. In contrast, QoS is specified as a measure of packet delay time, bit error rate, packets lost, economic cost of transmission or transmission power. Environmental, economic and application determine the appropriate network topology and routing algorithm. Three distinct network communication topologies exist for WSNs including star, mesh and a hybrid star-mesh.

Single-hop (star/direct): All nodes use single-hop communication directly to a single hub node as illustrated in figure 2.4(a). This topology benefits from its simplicity and ability to operate with low power consumption because of the simple data routing requirements. Star topology requires that every sensing node is in direct communication range of the hub node. This makes the topology vulnerable for large scale WSNs because communication paths can often become severely attenuated or blocked, especially in complex, obstructed environments such as indoors. This topology is one of the simplest network topologies and the ability for sensing devices to self-localize is impractical because those nodes only have a single-link communication to a hub-node and are reduced in function. However, a separate additional architecture could be used to estimate their positions by a method known as time-difference-of-arrival (TDOA).

Multi-hop (mesh/peer-to-peer): All nodes within radio range can communicate as illustrated in figure 2.4(b). Sensing nodes are normally symmetrical with respect to hardware, architecture and processing capabilities, therefore the topology is often referred to as peer-to-peer. The topology benefits from redundancy, scalability (network size $>$ transmission range using multi-hop) and robustness since there are often multiple routing paths between nodes and multi-hop communication capabilities are supported where intermediate nodes between a source and destination can be used to convey information [27]. However, high power consumption because of the complex routing algorithms required and network traffic resulting in processing latency can be a problem for mesh networks limiting the life expectancy of the network. This topology supports both fixed



(a) Single-hop (star). (b) Multi-hop (mesh). (c) Clustered multi-hop (hybrid star-mesh).

FIGURE 2.4: Wireless network communication and data routing topologies. Black circle: Reduced function device, White circle: Co-ordinator.

referencing and relative localization capabilities where sensing nodes may be designated as references, co-ordinators and 'blind' devices. It is important to note with this architecture that every device has symmetrical architecture and thus sensor nodes must be equipt with transceiver capabilities, a requirement of some ranging techniques.

Clustered multi-hop (hybrid star-mesh): The hybrid between a star and mesh network topology is illustrated in figure 2.4(c). This topology enables both simplicity and robustness with the advantage of reducing average power consumption. The network is divided into clusters where co-ordinator nodes communicate with cluster heads. Low power sensing nodes are not enabled with multi-hop capabilities but nodes designated as co-ordinators have the ability to forward data. From a perspective of localization, only co-ordinator devices could be localized in this architecture because sensing nodes only have single link communication; however it is worth noting that this topology resembles that of a mesh network in the conditions of signal blockage where nodes are reduced to only single link communications in some cases.

By analysis of network topologies, any ranging technique selected for sensing applications must fit the constraints of simplicity, low hardware overheads and be adaptable to all network topologies. The complexity of clustered multi-hop topology illustrates well why RSSI ranging is incorporated in the Zigbee stack because of its low complexity and non-interfering operation during data communication and routing. Zigbee supports the described networking topologies and specifies sensor nodes by three categories including: (1) full-functional device (FFD) ; (2) reduced-function device (RFD) ; (3) Personal area network PAN co-ordinator to meet the said network topologies. RFDs have no routing capabilities and can communicate only with PAN co-ordinators. Examples of RFDs include sensor nodes to monitor parameters such as temperature, humidity, vibration and motion. In contrast, FFDs have full networking capabilities and are suitable for self-configuring WSNs. A comprehensive reading of Zigbee network topology and devices is found in [35, 36], however, those are summarized herein as they involve the higher layers of the Zigbee stack that are considered outside the scope of this research.

Network topology and data routing are complex problems for large-scale wireless sensing applications because networks have limited resources, processing capabilities and power. The choice of network topology is dependent on the application of the wireless sensing system and any ranging or localization system must be adaptable to all of the aforementioned network topologies. For those reasons, ranging and localization methods must be simple and operate without interfering with data transfer and routing or increase latency while providing accurate and high resolution position estimation of sensing devices. Thus, any successful ranging and localization system for WSNs should either function in conjunction with data transfer between sensing nodes or by the use of a different transmitting channel. Ranging should use the readily available hardware to reduce overheads including power consumption, cost and complexity and physical size of the sensor node.

2.2.2 Communication Protocol

The communications protocol defines the PHY and MAC layers of the protocol stack. There are a wide variety of low power, fully integrated radio modules, including those from companies such as Atmel, Texas Instruments, MicroChip, Micrel and Mellexis which use different types of communications protocols. Those vary in terms of data transfer rate, power consumption, range and application. Typical wireless sensing applications require low rate ($<$ 250 kps) communications that must operate with the key constraint of low power consumption. The two wireless communications protocols that meet those fundamental constraints are IEEE 802.15.1 (Bluetooth) and IEEE 804.15.4.

Bluetooth (IEEE 802.15.1 and .2): Bluetooth was developed in 1999 by the wireless local area network (WLAN) working group [39] aimed at providing low-power, low-cost, short range, small size and a medium data rate communication. It is a personal area network (PAN) standard that operates with lower power consumption than IEEE 802.11. The maximum transmission power is limited to below one watt with a nominal bandwidth of 1 MHz for each of the 79 available channels. The standard originally served wireless communication over short range (i.e. personal space 0.0 m - 10.0 m) from personal computers to peripheral devices such as mobile phones, printers, digital cameras and personal digital assistants (PDAs) . Embedded Bluetooth capability has become widely used in many of those applications and is now an open standard which may be used freely. The transmission range of Bluetooth devices are defined by their class. Class one devices have operational ranges of greater than 100.0 m through the use of additional amplification. Class two devices have transmission ranges of 10.0 m - 100.0 m and class three devices transmit less than 10.0 m. Bluetooth uses a star network topology that supports up to seven remote nodes communicating with a single base station. Bluetooth transceivers operate using a combine Gaussian Frequency Shift Keying (GFSK) modulation and Frequency Hopping Spread Spectrum (FHSS) in the

unlicensed 2.4 GHz ISM frequency band. The specification states at transmissions must pseudo-random hop at 1600 times per second over at least 75 of the 79 available channels. Furthermore, compliant devices cannot operate on a given channel for longer than 0.4 s within any 30.0 s period in order to limit the amount of interference in the ISM frequency which is also used by the IEEE 802.11 standard. While some companies have built wireless sensors based on Bluetooth, they have not met with wide acceptance due to limitations of the Bluetooth protocol including: 1) Relatively high power for short transmission range; 2) nodes take a long time to synchronize to network when returning from sleep mode which increases average power usage; 3) low number of nodes per network (<=7 nodes per piconet); 4) MAC layer is overly complex when compared to that required for wireless sensor applications.

IEEE 802.15.4: The IEEE 802.15.4 Low-Rate WPAN (LR-WPAN) standard was specifically designed for the requirements of wireless sensing applications. The requirements include low-complexity, low-cost and low-power wireless connectivity for inexpensive devices covering applications outside the scope of the high data-rate WPAN. The standard is flexible with three defined PHY layers including the ISM 868 MHz, 915 MHz - 928 MHz and ISM 2.48 GHz - 2.50 GHz frequency bands. Data rates are 20 kbps (868 MHz band), 40 kbps (915 MHz - 928 MHz band) and 250 kbps (2.48 GHz - 2.50 GHz band) respectively. There are 10 channels available in the 868 MHz and 915 MHz frequency bands and 16 channels available in the 2.48 GHz - 2.50 GHz frequency band. While the 868 MHz and 915 Mhz bands are only available in Europe and North America, the 2.48 GHz - 2.50 GHz band can be used freely world-wide and for this reason, has become the most accepted frequency band for IEEE 802.15.4. The 868 MHz and 915 MHZ - 928 MHz frequency bands operate using a binary phase shift keying (BPSK) modulation and an offset quadrature phase shift keying (O-QPSK) scheme is used for the 2.48 GHz - 2.50 GHz band. Both also employ direct sequence spread spectrum (DSSS) . The data communications rate of IEEE 802.15.4 is low in comparison to that of Bluetooth in order to reduce power consumption, a key requirement of wireless sensing applications. This is complemented by power saving features including sleep mode designed to reduce power consumption when the sensing device is inactive. When a sensor node wakes up from sleep mode, rapid synchronization to the network can be achieved. This capability allows for very low average power supply current when the radio can be periodically turned off. The standard details specifications of the PHY and MAC layers capable of offering building blocks for different network topologies including star, mesh and star-mesh. Network routing schemes are designed to ensure power conservation and low latency through guaranteed time slots.

The standard also benefits from optional Advanced Encription Standard AES-128 security of transmitted data and link quality indication (LQI) , useful for multi-hop mesh networking algorithms. IEEE 802.15.4 is expected to become the most widely accepted standard for wireless sensing applications mainly because of the low-power features it

can offer. The high radio date rates achievable in the 2.48 GHz - 2.50 GHz frequency band also reduce frame transmission time and thus the power consumption per transmitted message compared to the lower 868 MHz and 915 MHz - 928 MHz frequency bands. Furthermore, the 2.48 GHz - 2.50 GHz band is essentially a worldwide license-free band.

IEEE 802.15.4 Frame format:

Frame structure has been designed to keep complexity to a minimum while making them sufficiently robust for transmission on a noisy channel. Each layer of the protocol stack adds to the frame structure with layer-specific headers and footers. LR-WPAN defines four types of frame structure including a beacon frame, data frame, acknowledgement frame and MAC command frame. The different types of IEEE 802.15.4 frame are similar in structure and only differ by the complexity of the PHY service data unit (PSDU). A full description of all four frame formats can be found in [29] but only the data frame format is considered herein due to its more suitable adaptability for ranging techniques. The data frame structure originates from the upper layers of the protocol stack and is illustrated in figure 2.5 as transmitted by the physical layer from left to right. The fields added by each layer of the protocol stack are shown along with their length in bytes. The PHY layer represents the bits that are actually transmitted on the physical medium. The packet structure or data frame consists of a synchronization header (SHR) , Physical (PHY) header and PHY service data unit (PSDU) . The synchronization header consists of a preamble sequence of 4 bytes followed by a single start-of-frame-delimiter (SFD) byte. During reception of a data packet, the synchronization header is used by the radio receiver signal demodulator to identify and synchronize (frequency adjust) to the incoming data frame. Thus, a continuous search and correlation process of the incoming packets preamble sequence is made with a local copy to identify IEEE 802.15.4 compliant packets. When a data packet is identified (i.e. the preamble matches the local copy), the start-of-frame delimiter enables the receiver to achieve symbol synchronization. The proceeding MAC protocol data unit (MPDU) can then be read by the receiving device following the PHR header which defines its length in bytes. The MPDU consists of a MAC header (MHR) , MAC payload and MAC footer (MFR) . The data payload is passed from the upper layers of the protocol stack to the MAC sub-layer where the MHR and MFR are appended. The MHR and MFR consist of the frame control, sequence number, addressing information of the packet and frame check sequence (FCS) . Full details of those functions can be found in [29]. The MHR, MSDU and MFR together form the MAC data frame (MPDU).

2.3 Ranging in WSNs

The estimate of distance to a remote point or target from a known observation point is known as ranging [40] and is a one-dimensional problem. In contrast, the estimation of

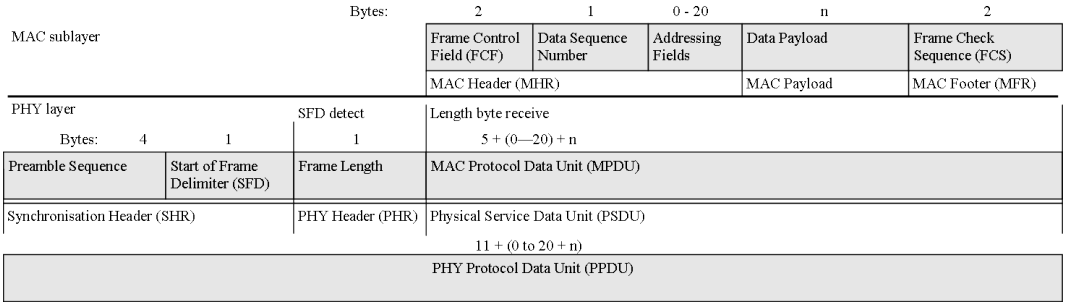


FIGURE 2.5: IEEE 802.15.4 data frame format [29].

a targets position by means of bearing measurements, angle measurements or multiple range estimates to or from more than one reference position is known as localization [41, 42, 43] and is a multi-dimensional problem. Ranging and localization techniques cannot be compared directly because they relate to the dimensional complexity of the problem and application of the system. Ranging techniques use properties of the wireless channel to estimate distance in contrast to Angle-of-Arrival (AOA) techniques which use direction and bearings of the received signal to estimate position. To consider ranging methods, there are three perspectives of the wireless channel including: 1) time domain view; 2) frequency domain amplitude view; 3) frequency domain phase view. A ranging signal transmitted through the wireless channel is described in the time-domain by x(t) or in the frequency domain by its Fourier transform X(f). Figure 2.6 illustrates the wireless channel as a simple block diagram with the key input and output parameters for both the time and frequency domain. In the time domain, the channel has a characteristic or *impulse response* h(t) and the corresponding signal received at the receiving device is y(t). From the frequency perspective, the wireless channel has a *frequency transfer function* H(f) with corresponding output Y(f). The wireless channel is normally considered to be *time-invariant* and *linear* to simplify both analysis and modelling. However, this is sometimes not the case and the channel must be considered as *time-variant* requiring more complex modelling or filtering for its representation. The time-invariant channel is categorised in the *Time Domain channel view* by its channel impulse response (CIR) h(t), which is the response when the input is equal to a unit impulse δ(t), that is h(t) = y(t) when x(t) = δ(t). The response of the propagation channel to an arbitrary input x(t) is found by the convolution of x(t) with h(t). Provided there is no output prior to time t=0, when the input is applied, the output y(t) may be expressed by equation 2.1 and is referred to as the convolution integral [44]. In the absence of signal reflections at the receiver, the CIR has a single filter tap as described by equation 2.2, where τ_0 is the direct LOS path and A is the signal amplitude [17].

$$y(t) = \int_0^\infty x(\tau)h(t-\tau)d\tau \tag{2.1}$$

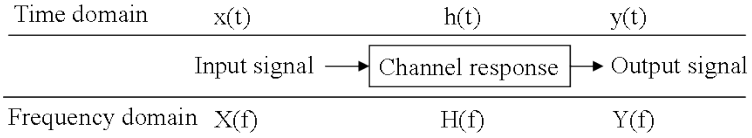


FIGURE 2.6: Time and frequency domain response illustration with key parameters.

$$h(t) = A \cdot \delta(t - \tau_0) \tag{2.2}$$

When a signal is attenuated in the direct path or reflected of obstacles, multiple signals arrive at the receiver with different delays, a phenomena called Multipath propagation. Therefore multiple taps appear in the CIR along the direct path tap [17]. Time of Arrival (TOA) and Time-Difference-of-Arrival (TDOA) ranging techniques use the time domain channel view [45, 17, 24, 13, 21]. Those systems utilise either acoustic signals, electromagnetic signals or both to measure TOA as explained in the proceeding sections. The *Frequency Domain Amplitude View* categorises the power attenuation due to the wireless channel. Since convolution in the time domain transforms to multiplication in the frequency domain, the frequency domain output signal response is $Y(f) = X(f)H(f)$ and channel frequency response is $H(f) = Y(f)/X(f)$, provided that $X(f) \neq 0$. The behaviour of Received Signal Strength (RSS) is described by the free space path loss model which will be explained in detail later. In its simplest form it may be described by equation 2.3 where d is the transmitter-receiver distance and β is the propagation factor. Equation 2.3 indicates that RSS typically decreases with increased transmitter-receiver distance with a non-linear relationship.

$$|H(f)| \propto \frac{1}{d^{\beta}} \tag{2.3}$$

As with the time domain perspective, when the direct signal path is attenuated and signals are reflected, multiple copies of the signal arrive at the receiver with different delays. Therefore the channel frequency response can interfere constructive or deconstructive by attenuating or amplifying the signal in its spectrum [17]. This indicates that the attenuation or reflection of a signal in the wireless channel is effected by the channels frequency response. The *Frequency Domain Phase View* uses the phase shift in the frequency response for range estimation [17]. This relationship is linear and defined by equation 2.4, where f_0 is the carrier frequency, t_0 is time and $\angle H(f)$ is the phase offset.

$$\angle H(f) = 2\pi f_0 \tau_0 \tag{2.4}$$

The frequency transfer of a time-invariant wireless channel can be measured by applying

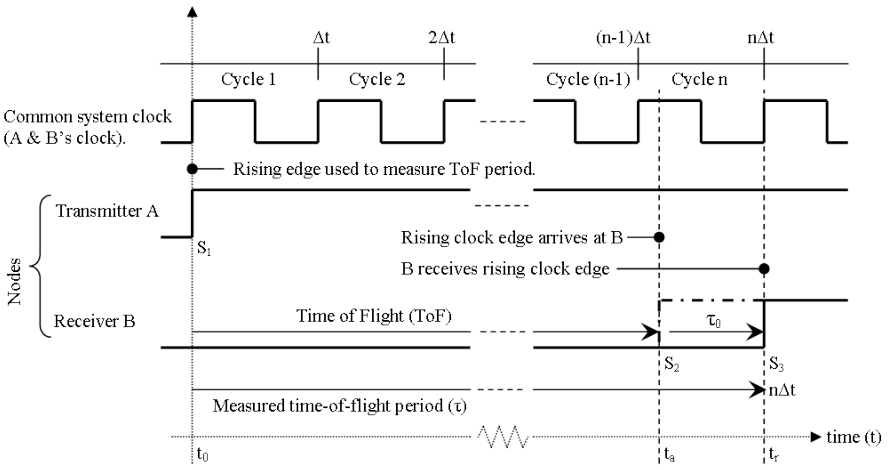


FIGURE 2.7: Timing diagram of synchronized TOF ranging between a transmitter A and receiver B using a common system clock.

a sinusoidal waveform to a transmitter and measuring the received signal phase offset $\angle H(f)$ at a receiving device at distance d[m] using an oscilloscope. The input sinusoidal wave is stepped through the available bandwidth and the phase offset of the output waveform is measured with respect to the input sinusoidal wave. As with the frequency domain amplitude view, the simple relationship between phase change and range suffer from attenuation in the wireless channel. Ranging systems using signal phase change for range estimation therefore operate at low frequencies ($<$ 1 kHz) to reduce the effects of signal reflections at the receiver. The phase measurement is extracted from the difference between the electric and magnetic parts of an electromagnetic signal and is known as Near Field Electromagnetic Ranging (NFER) [46].

Time of Arrival Ranging

Time-Of-Arrival (TOA) ranging involves the measurement of the transit time of an acoustic or electromagnetic signal from a known observation point to a remote object in order to estimate the distance. It may be assumed that electromagnetic or acoustic signals travel with constant or uniform velocity in straight lines making a change in displacement Δs over a change in time Δt between two points. The average velocity v of the electromagnetic or acoustic signal is described by the relationship $v = \Delta s/\Delta t$, and in the limit, using calculus notation v (ms^{-1}) $= \delta s/\delta t$. Velocity may be defined as the rate of change of displacement (position), where $\delta s/\delta t$ is the instantaneous velocity at the time or place concerned. Velocity is a vector physical quantity and both the scalar absolute magnitude (speed) and direction of motion are required for its definition [47]. It can easily be seen from the equation $v = \delta s/\delta t$ that the distance-time relationship is linear and the distance estimate is computed after the transit time is obtained. The speed of propagation of electromagnetic waves through any medium is defined by c_{ele} (ms^{-1}) $= 1/(\sqrt{\epsilon\mu})$, where μ is the permeability and ϵ is the permittivity of the medium. In free space, $\mu_0 = 4\pi$ x 10^{-7} Hm^{-1}, $\epsilon_0 = 8.85$ x 10^{-12} Fm^{-1}, so $c = 299792458$ ms^{-1},

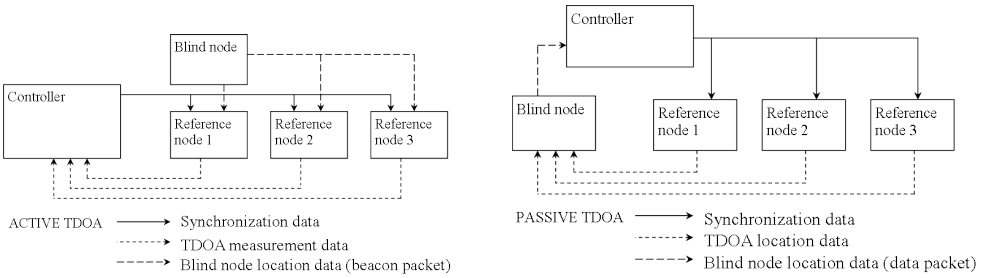
or more approximately 3.0 x 10^8 ms^{-1} [48]. Throughout this work, unless otherwise stated, it is assumed that all electromagnetic waves travel at the same speed through free space and the speed of signal propagation is 3.0 x 10^8 ms^{-1}. In contrast, the speed of an acoustic signal c_{aco} in a solid medium is defined as $c_{aco} = \sqrt{E/\rho}$, where E $[Nm^{-2}]$ is the modulus of elasticity and ρ $[kgm^{-3}]$ is the density of the medium [47]. In free-space, the speed of acoustic signals are defined as $c_{aco}ms^{-1} = \sqrt{\zeta E/\rho}$, where ζ is the ratio of the molar heat capacities of the gas. For air, $\zeta = 1.40$, $E = 1.10$ x 10^5 Nm^{-2} and $\rho = 1.29$ kgm^{-3}. The speed of acoustic signals in free-space assuming an ambient temperature of Celsius is therefore 331 ms^{-1}. Acoustic signals propagate significantly slower than electromagnetic signals, therefore the requirement of fast processing capabilities to resolve timing estimates are reduced. For example, range measurements in WSNs are required with resolution 0.3 m. By using electromagnetic signals to estimate TOA, this requires timing capabilities in excess of nanoseconds. Alternately, if acoustic signals are used, timing requirements in excess of milliseconds are required based on free space propagation which is significantly easier to achieve in comparison to electromagnetic signal timing requirements. The use of slower signal propagation speeds for TOA also reduce power requirements and synchronization thresholds between the transmitting and receiving devices. However, acoustic ranging has several drawbacks, highly directional and expensive transducers are required which are less energy efficient than the wireless communication links already adapted on sensor nodes. Equipping every wireless sensing node with a transducer is both expensive and a large overhead when considering additional power consumption and hardware alone. Therefore the use of acoustic or electromagnetic TOA ranging is a choice dependent on parameters including hardware overheads, cost, complexity and scalability of the WSN in question. Acoustic ranging methods have also demonstrated less resilience to multipath signal propagation in comparison to electromagnetic TOA ranging systems.

Ranging by one-way TOA is illustrated from the time perspective in figure 2.7 for a single ranging transaction between a transmitting device A and receiving device B which are precisely synchronized to a common system clock with period Δt. In essence, one-way ranging determines the range between the devices by measuring the one-way duration of time (TOF) required for a signal to travel from device A to device B. For the purpose of explanation, it is assumed that a rising clock edge is used for TOA estimation which is transmitted from A at time t_0 (S_1) with known transmit time in order for receiver B to estimate the TOF period at S_3. Since B is a digital device, TOF signals can only be received on rising clock edges and hence the quantization error τ_0 exists. For this reason, if a ranging signal arrives at B at S_2, B detects this ranging signal at S_3 after n clock periods. The signal propagation period, with resolution Δt, can then be determined by subtracting the time of transmission from the TOA. The distance estimate is then computed using $\Delta s = v\Delta t$. TOA estimates are modelled in terms of the contribution of the distance estimate d_i, the transmitter-receiver clock offset and an error component caused by noise, multipath and receiver processing delays. Assuming

the TOA errors are independent and identically distributed random variables, then a single ranging observation is a zero-mean Gaussian distributed random variable mean d_i and variance σ^2. Therefore TOA ranging estimates are described by $\hat{d}_i = d_i + n(0, \sigma)$, where $\hat{d}_i$ is the estimated range [49]. This agrees with [50] which reports that the accuracy of TOA estimates are improved by averaging multiple measurements, hence reducing the variance of the final TOA estimate. The Cramer-Rao lower bound detailed in the proceeding chapter is commonly used to model for the lower bound accuracy of TOA estimates. This relates the signal bandwidth and Signal-to-Noise Ratio (SNR) for a given TOA system to its expected performance.

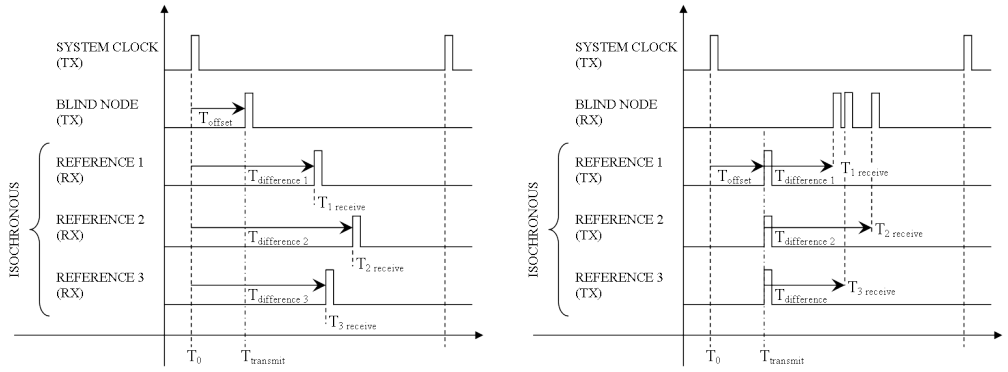
Time Difference Of Arrival

In some circumstances, equipting sensor nodes with transceiver capabilities is either uneconomic or impractical. A radio-frequency identification system where location information is required is a good example where the tag must be low cost because of the possible large volumes of use, simple in both hardware and software complexity in order to meet low cost and operate only with current induced through a coil because onboard batteries are not included. Time-difference-of-arrival (TDOA) systems are suitable in these circumstances [24]. TDOA uses a set of synchronized reference nodes at known positions in order to determine the TDOA of ranging signals to or from a blind device for localization. Implementation of TDOA is achieved using one-way TOA ranging by either active or passive architectures as illustrated in Figure 2.8. The corresponding timing diagrams are shown in Figure 2.9. In passive TDOA, a blind node receives multiple ranging signals from reference nodes and determines the TDOA based on knowledge of the reference node positions. Alternately, in active tdoa, a blind node transmits a beacon ranging signal which is received by multiple reference nodes and is used to compute the blind nodes position. Active TDOA is more commonly used because it meets the key constraints of tags or blind devices only requiring transmit capabilities, therefore requiring less hardware complexity and power for operation. The reference components are static and synchronization may be achieved through a number of wired or wireless techniques. Either an external system clock co-ordinator or periodic beacon signal broadcast from a dedicated system clock may be used. Synchronization must be absolute and reference nodes must know their precise positions relative to the beacon provider. The performance of TDOA systems is reported to be very dependent on the time precision of the synchronization pulse. TDOA systems are unable to measure the TOA of a signal from a transmitter to a receiver directly because these two system components are unsynchronized. An unknown time offset exists between the clock on the device to be located and the referencing architecture [24]. For this reason, instead of converting the TOA of the ranging signals at a receiver into a transmitter-receiver range, the receivers in a TDOA system convert the TOA into a first-approximation pseudorange (by multiplication by the speed of signal propagation). The pseudorange encapsulates both the range and clock offset information.



(a) Active time-difference-of-arrival. (b) Passive time-difference-of-arrival.

FIGURE 2.8: Time-difference-of-arrival architectures using one-way ranging transaction.



(a) Active time-difference-of-arrival timing. (b) Passive time-difference-of-arrival timing.

FIGURE 2.9: Timing diagrams for time-difference-of-arrival passive and active architectures.

The position estimate of a blind device is computed using a non-linear model if applied to multiple pseudoranges to a number of known reference points using TDOA. The non-linear model for a two-dimensional TDOA system is denoted by equation 2.5, where (x_i, y_i) is the position of the ith known point, p_i is the pseudorange between the object and the ith known point, (u, v) is the estimate of the objects location, c is the speed of signal propagation, t_{ck} is the unknown transmitter-receiver clock offset, and ϵ_i is a term which accounts for the errors in the fitted model. Note that TDOA systems must estimate an additional unknown parameter, the clock offset in comparison to TOA locating systems and therefore TDOA systems must measure at least one more pseudorange than the equivalent TOA system [24].

$$p_i = \sqrt{(x_i - u)^2 + (y_i - v)^2} + c.t + \epsilon_i (i = 1, ..., n),) \tag{2.5}$$

The Global Positioning System (GPS) is a good example of a TDOA positioning system. GPS utilises one-way time-difference-of-arrival (TDOA) ranging where both the satellites and receiver clocks are loosely synchronized. Satellites are synchronized to a common

GPS time base and the user GPS receiver operates from an unsynchronized crystal clock normally employed to minimize cost, complexity and size. Other implementations of TDOA include cell phone locating, navigational and asset locating systems and the Loran C system, [21, 51]. However, as with TOA, TDOA measurements are also degraded by channel impairments, circuit and logic delay and manufacturing tolerances. TDOA has been particularly suited in locating systems using UWB technology to enable precise positioning for indoor applications [21].

Received Signal Strength

Radio signals are attenuated by the path loss of the wireless channel and this phenomena can be used to estimate the range between a transmitter and receiver. The received signal strength (RSS) decreases exponentially with linear increase in transmitter-receiver separation distance. The receiver must measure this attenuation to estimate the transmitter-receiver distance which requires both a zero-distance calibration and a model to describe the log-normal characteristic of the wireless channel. Modelling the wireless channel is a complex problem because of the diverse range of environments such as indoor, offices and partitioned spaces. Reflection and attenuation of signals interfere both constructively and deconstructively with RSS measurement [52, 53, 54]. The logarithmic power decrease must therefore be extracted from fast, medium and slow fading channel attenuation components illustrated by figure 2.10. Fast fading components occur from the presence of obstacles which reflect signals. The effect of those components can be reduced through filtering, time averaging or spread-spectrum (SS) signal modulation techniques [18, 55]. In contrast, medium and slow fading components occur from the propagation of the signal through objects, terrain contours and noise, however, knowledge of the surrounding environment is required to remove those errors and ambiguities in order to meet the accuracy and resolution requirements of WSNs. Wireless channel propagation models that closely resemble the true environment are therefore a fundamental requirement of RSS ranging systems. One of the simplest models to describe this behaviour is the Fritts transmission equation 2.6. This model describes the propagation of an electromagnetic signal in free space with the assumptions of direct-path LOS propagation and no signal reflections [50].

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi d})^2 \tag{2.6}$$

The term $(\frac{\lambda}{4\pi d})^2$ defines the path loss where d is the range separation between the transmitter and receiver, G_t and G_r are the power gains of the transmitter and receiver antennas, P_t, P_r are the transmit and receive powers and λ is the carrier signal wavelength [56]. Equation 2.6 illustrates two important points about the characteristic of RSS measurements. There is an inverse square law relationship between power loss and transmitter-receiver distance. The presence of the carrier wavelength λ implies that path loss in free space is frequency dependent. This frequency dependence is explicitly

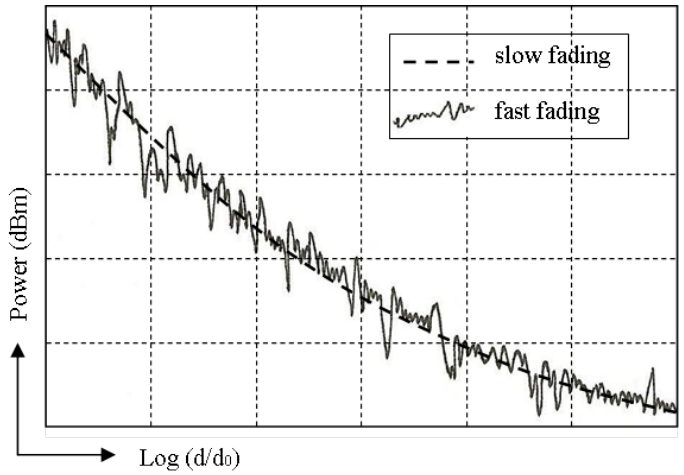


FIGURE 2.10: Example of fading components of received signal strength indication (RSSI).

TABLE 2.2: Reported path loss exponent values γ for different environments [57].

Environment	γ range
Urban canyon	2.7 - 6.5
Office building	1.6 - 3.5
Office building (multiple floors)	2.0 - 6.0
Industrial environment	1.6 - 3.3
Residential dwelling	3.0 - 3.5

introduced by the effects of the transmitter and receiver antennas and can be seen by performing LOS RSS measurements using UWB signals with different antennas [50]. Path loss is however not frequency dependent in free space because all antennas transmit their power flux density (Φ) spherically over distance d ($\Phi = (\frac{P_t}{4\pi d^2})$ varying as $1/d^2$. The frequency dependence characteristic of the antennas must however be acknowledged [57]. The non-linear characteristic of RSS measurements has been verified by research which shows that path loss increases logarithmically with linear increase in transmitter-receiver distance. For this reason, the log-normal path-loss model for the fading channel is a widely accepted estimator for the mean channel path loss described by equation 2.7 and 2.9.

$$\overline{P}_L(d) \propto \left(\frac{d}{d_0}\right)^{\gamma} \tag{2.7}$$

$$P_r = P_t k \left(\frac{d_0}{d}\right)^{\gamma} \tag{2.8}$$

The mean path loss is $\overline{P}_L(d)$, d_0 is the zero-reference transmitter-receiver distance, d is the separation distance and γ is the path loss exponent. The path loss exponent

γ represents the rate of increasing path loss with distance and is dependent on the environment. Reported values of γ are summarized in table 2.2. Frequency dependence can enter equation 2.9 through the path loss exponent γ due to the diffraction, scattering and material penetration of signals [50]. However, its has been reported that frequency dependent behaviour is not experienced at short range ($<$ 10 m). For this reason, the model is only valid for transmission distances of 1 m - 10 m indoors and 10 m - 100 m outdoors [50]. Extensions of the free-space log-normal path loss model include the two-way model, kata model and the COST extension to the Hata model. Received power at any distance can be calculated by equation 2.9 where the frequency dependence due to the antenna effects is included entirely in the reference measurement P_t, received at a close proximity reference distance, where k is a unitless constant that depends on the antenna characteristics and channel attenuation. The unitless constant is determined by measurement at zero-distance d_0 or optimized with γ to minimize the mean square error between the model and empirical measurements. This combined measurement is denoted by η and the received power P_r is more simply represented in terms of the transmit power P_t by equation 2.9.

$$P_r = P_t 10\eta log_{10}\left(\frac{d}{d_0}\right) \tag{2.9}$$

In the presence of error due to medium scale fading, the measured power $\hat{P}_r$ includes a random noise contribution X_σ ($\hat{P}_r = p_r + X_\sigma$). The noise contribution representing medium scale fading in the channel and is typically reported to be zero-mean and normal (in dB) with variance σ^2_{dB} invariant with range [58]. Small scale error contributions can be neglected since it can be assumed that time-averaging or spread-spectrum techniques are employed and thus do not interfere with the distribution of X_σ from the log-normal distribution of the medium-scale fading. Equation 2.9 can be re-written to include a noise contribution X_σ denoted by equation 2.10.

$$P_r = P_t 10\eta log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{2.10}$$

Equation 2.10 illustrates that the accuracy of RSS range estimates are degraded with increasing transmitter-receiver separation distance. Thus, at large separation distance ($>$ 40 m), the power of the noise contribution X_σ becomes significant ($X_\sigma > P_t 10\eta log_{10}(\frac{d}{d_0})$) and range estimates become severely degraded. For this reason, RSS ranging can only operate well when ranging is performed well below the transmission range of the radios to prevent large range estimate errors through the contribution of noise. This makes RSS ranging more suitable for dense sensor networks where inter-device distances are well below the transmission range of the radios. RSS ranging also benifits from less hardware overheads in comparison to TOA and TDOA ranging systems and also does not require the precise synchronization of independent devices. Similar to NFER, only a

single receiver is required to estimate range. Wireless standards including IEEE 802.11 and IEEE 802.15.4 support RSS ranging. On reception of a data packet, the RSS range estimate is extracted through the MAC layer as an eight-bit binary value [55]. The measurement is filtered over eight symbol periods to reduce the contribution of error in the estimate from multipath and attenuation factors and the receiver converts the logarithmic relationship of received power to a linear estimate-distance relationship with a dynamic range of 100 dBs [55]. Calibration of the zero-distance estimate is also performed internally by the radio module. RSS range has been reported to operate well at short range, ranging accuracy better than ± 1.0 m has been demonstrated below 5.0 m [58].

Near Field Electromagnetic Ranging

Radio-frequency signals consist of both and electric and magnetic component. At close proximity of a transmitting antenna (< 0.1 m), the electric and magnetic components of the RF signal have phase difference $\pi/2$ rad s^{-1}. This phase difference converges with increased distance from the transmitter. Therefore, by independently detecting and measuring the phase difference between the electric and magnetic components of the RF signal [59], a range estimate is obtained. NFER has no synchronization requirements between the transmitting and receiving device and range measurement is obtained using only a single receiver. In addition, as the electromagnetic phase differences are preserved when a signal is down converted to base-band, the required ranging accuracy of WSNs can be achieved with relatively low timing requirements (in the region of microseconds). The relationship between the electric and magnetic signal components is described by equation 2.11 where Δ_Φ is the phase angle between the electric and magnetic component and $\hat{d}$ is the estimated range. The corresponding characteristic is illustrated in figure 2.11.

$$\hat{d} = \frac{\lambda}{2\pi} \sqrt[3]{cot\Delta_\Phi} \tag{2.11}$$

NFER operating within a half-wavelength to avoid aliasing of the phase measurement Δ_Φ requires very low frequency operation (100 m range $\rightarrow$ λ = 200 m $\rightarrow$ f = 1.5 MHz). Low frequency signals are on average more penetrating than high frequencies. In addition, low frequencies are more immune to multipath interference. NFER therefore has superior characteristics in obstructed conditions such as indoors and multipath environments in comparison to LAN/WLAN standards which operate at much higher frequencies. In contrast, NFER systems suffer from phase offset introduced by materials creating relatively gradual phase shifts. The 530 kHz - 1710 kHz low frequency Amplitude Modulation (AM) broadcast band has been allocated for its use. However, its ranging operation in this frequency band must comply with FFC regulations which limit a maximum transmission power to 100 mW. The operating range of NFER locating systems is therefore limited to short range (<60 m) indoor applications [59]. The

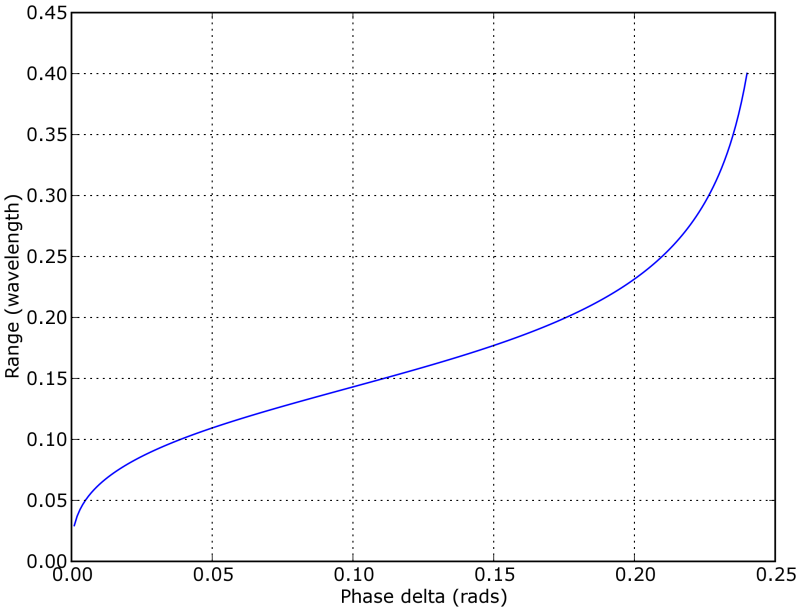


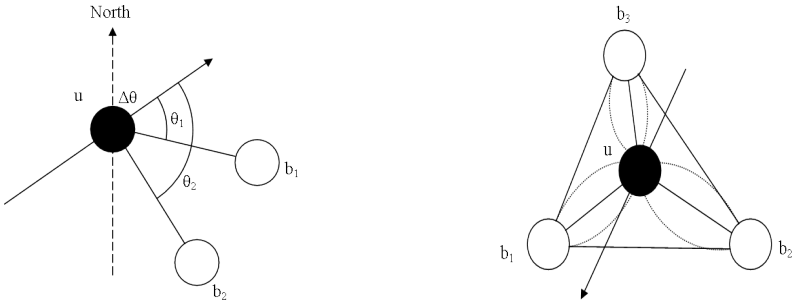
FIGURE 2.11: The phase change delta between the electric and magnetic phase components provides useful range information within about one third of a wavelength of an electrically small antenna [59].

use of low frequency also has practical antenna considerations. Antennas are most efficient when the signal wavelength is comparable to the dimensions of the antenna. High frequencies (i.e. 2.4 GHz) require smaller antennas than low frequency signals (i.e. 1 kHz). The impractically large size antenna required for a NFER system (λ = v/f = 300000 m) is a significant problem for sensor nodes which are small in physical size ($>$ 0.1 m^3). NFER is an emerging ranging method suitable for real-time locating in complicated indoor propagation environments [59]. Tracking accuracy better than $\pm$ 0.6 m has been demonstrated using tags transmitting unmodulated RF tones and locator receivers spaced by 55.0 m [59].

Angle of Arrival Localization

Angle of Arrival (AOA) localization involves the use of antenna arrays on receiving devices to measure the orientation of incident signals with respect to a reference direction, a technique known as triangulation [60]. Orientation, defined as a fixed direction against which the AOAs are measured, is represented in degrees in a clockwise direction from north. When the orientation is zero degrees or pointing to the north, the AOA is absolute, otherwise relative. By using two-dimensional antenna arrays, a single receiver unit can determine bearings of the signal transmitter in both azimuth and elevation [24]. Bearing can also be combined with distance estimates or other angle measurements to operate as a hybrid system [22]. However, current wireless standards do not incorporate AOA for localization. AOA is an alternative localization approach, unlike ranging methods which use properties of the received signal to estimate distance. The angle of

received signals from two or more locations is measured using a complex phased array antenna. Complex antenna arrays are both expensive and large in physical size when considered for wireless sensing applications. Furthermore, AOA based locating systems have been reported to suffer in both multipath and NLOS environments. The localization process using AOA is solved using triangulation as illustarted by Figures 2.12(a) and 2.12(b). Figure 2.12(a) illustrates signals arriving with angles θ_1 and θ_2 measured at unknown u, transmitted from references b_1 and b_2. Assuming the orientation of the unknown is $\Delta\theta$, the absolute AOAs from b_1 and b_2 are calculated as $(\theta_i + \Delta\theta)(mod 2\pi)$, $i = 1, 2$. Each absolute AOA measurement corresponding to a beacon restricts the location of the unknown along a ray starting at the beacon. The location of the unknown u is located at the intersection of all the rays when two or more non-collinear beacons are available, in other words, when the absolute AOAs cannot be obtained, the AOA differences can be used instead. In Figure 2.12(b), angles $\angle b_1 u b_2$, $\angle b_1 u b_3$ and $\angle b_2 u b_3$ can be computed using the knowledge of the relative AOAs. All angles subtended by the same cord are equal. Thus, given two points and the chord joining them, a third point from which the chord subtends a fixed angle is constrained to an arc of a circle. The angle $\angle b_1 u b_2$ and the chord $b_1 b_2$ restrict $u's$ position on the arc passing through b_1, u and b_2. Since each chord determines one arc, the location of an unknown is at the intersection of all arcs when three or more non-collinear references are available [60]. At least two non-collinear reference points are required to discover the location when the orientations are known, and at least three to discover both the location and the orientation. AOA is susceptible to error if blind devices do not receive angle measurements from a required number of references. Error in AOA measurements are also caused by both channel imparments and the hardware used to estimate the AOA. The spatial properties of the wireless channel have significant impact on the detection of AOA [60]. A considerable effort has been dedicated to finding good models to characterise these properties [60, 61]. However, the distribution of AOA measurements is very dependent on the communication environment, therefore a single model which can perform well in all scenarios is difficult to achieve. The existence of sub-components within impulse response measurements has been recognised for mobile radio propagation. In previous work [60], Cox has shown that multipath sub-components could arrive at the receiver from many directions even though their differential propagation delays were small. Investigation into the angles of arrival for indoor radio multipath propagation has also demonstrated that multipath components with temporal resolutions of approximately 25 ns contain sub-components arriving from different angles of arrival. However, AOA ranging may be improved by exchanging AOA measurements with neighbouring nodes, and the relative AOA with respect to each beacon (even multiple hops away) can be calculated based on geometry relations among the nodes.



(a) Localization with orientation information.

(b) Localization without orientation information.

FIGURE 2.12: Triangulation in AOA localization with and without orientation information. [62].

2.4 Discussion

Sensor nodes within WSNs are often deployed without a prior knowledge of their location and a method to estimate their absolute or relative positions is required to provide additional information to the quantity being measured. In this chapter, we have summarized WSNs and methods of estimating distance or orientation between those sensing nodes in order to determine their relative separation distances and positions. Wireless sensing nodes have a diverse range of applications in many monitoring, control and tracking applications and thus they have been standardized by, application hardware, communication protocol, network capabilities and software architecture.

There are five methods that can be used to estimate the range between sensor nodes, these include Time-Of-Arrival (TOA), Time-Difference-Of-Arrival (TDOA), Received-Signal-Strength (RSS), Near-Field-Electromagnetic-Ranging (NFER) and Angle-Of-Arrival (AOA).

AOA involves the use of complex antenna arrays to measure the arrival angle of a received signal. The requirement of complex antenna arrays make AOA an impractical solution for sensor nodes due the physical size of those antennas [17], additional hardware overheads and power consumption.

TDOA uses a set of synchronized reference nodes at known positions to localize a blind device by estimating the TDOA between the ranging signals to or from the referencing devices. The referencing architecture requires wired infrastructure to meet the synchronization and data transfer of TDOA measurements. This is a costly overhead and limits TDOA applications to fixed referencing architectures. In addition, the blind device in question must have direct-link communication to at least four references. This is a constraint that is not always possible in WSNs because of the diverse range of applications.

NFER involves the measurement of the phase change of a signals magnetic and electric component to estimate distance. NFER operates on very low frequencies (within the

AM broadcast band 530 kHz - 1710 kHz) hence benefiting exhibiting propagation properties. However, as with UWB based TOA ranging, this technique can interfere with other systems and therefore the Federal Communications Commission (FCC) limit the maximum transmission power. For this reason, UWB based TOA and NFER ranging methods can only operate over short range (< 60 m) [59].

RSS involves measuring the attenuation of a signal through the wireless channel to estimate the transmitter-receiver distance. The simplicity and low hardware overheads of this technique have led to its implementation on many WSN hardware platforms. RSS measurements are often readily available from the communication radio [55], however, the consistency of range estimate accuracy can be very unreliable due to complex propagation environments and multipath. Those effects can be removed by employing complex models of the propagation environment, however, a generalize model is difficult to produce because every propagation environment has different characteristics. RSS ranging is also very limited in range due to its log-normal range estimation characteristic. It is therefore more suitable for short range applications (< 40 m) in comparison to TOA, TDOA, NFER and AOA ranging methods. Furthermore, RSS locating systems are reported to be less suitable for precise locating as discussed in chapter 1.

TOA ranging involves the measurement of the transit time of a signal to estimate distance and has a linear distance-range estimate relationship. The method has demonstrated its ability to operate well in high multipath environments and provide sub-metre range estimates using Ultra-wideband (UWB) technology [13]. However, this has been through the use of a TDOA architecture where wired infrastructure between a set of references to meet the synchronization is a requirement [21]. To meet the synchronization requirements of TOA ranging without this wired infrastructure requires ranging to be performed very quickly and both the transmitting and receiving device system clocks to be very accurate. This would be challenging to implement on sensor nodes which operate from crystal oscillator clocks that are not precise (accuracy $< \pm 40$ ppm). The transmission power and signal bandwidth of UWB technologies are also regulated by the FCC limiting their application to short range (< 60 m). Sensor nodes are resource constrained and low complexity, thus the implementation of precise measuring equipment is impractical. The error in TOA estimates could be reduced by using low Parts-Per-Million (PPM) crystal oscillators [58] however this would increase the cost of sensor nodes. Alternative research has demonstrated the use of both RF and acoustic capabilities to mitigate the synchronization requirement and enable TOA ranging on sensor nodes. However, acoustic signals are directional and require unobstructed direct path signal propagation for high performance range estimates. They also rely on expensive, high power transducers which are an over head in terms of power consumption for sensor nodes. Those problems can be mitigated by using two-way TOA ranging, a technique originally used in long range applications where response delays were considered negligible and signal propagation was direct-path LOS in free-space, thus the effects of

multipath interference are insignificant.

Ranging in WSNs is challenging because of the constraints of sensor nodes in terms of power consumption, hardware overheads and low processing capabilities and the accuracy and resolution requirements of the localization mechanism. Ranging accuracy is required better than $\pm$ 1.0 m using simple hardware and resource constrained sensor nodes with low power operation ($<$ 27 mA transmit, 25 mA receive using 2.0 V - 3.6 V supply in active mode [55]). Those sensor nodes also operate in an unsynchronized manner from inaccurate low frequency crystal device clocks (32 kHz - 32 MHz, $C_0 \pm 40$ ppm without temperature compensation [55]). In addition to the technical challenges, low cost and physical size limitations also set stiff constraints. Ranging must operate within those constraints using computationally simple algorithms and also be adaptable to the standardized software stack and communication protocol. For those reasons, RSS and TOA are suitable techniques which can operate with the use of existing sensor hardware and communication protocol. In comparison, TDOA, AOA and NFER would require either additional infrastructure or hardware overheads and are likely to increase power consumption.

IEEE 802.15.4 standardizes the design of LR-WPANs physical and MAC layers, which are suited to wireless sensing applications and thus the ranging system should also be both adaptable and compatible with this standard. It is beneficial to perform and extract range measurement and position information both without disrupting data communication and channel bandwidth. The standard is more commonly using the 2.4 GHz frequency band for data communication mainly because of the wide range of single-chip devices that operate in this frequency band. Therefore ranging utilising this frequency band is both adaptable to current standards and can be combined to reduce power consumption and additional communication bandwidth overheads. To meet the low power requirements of WSNs, typically which can be achieve mainly through low duty cycle operation of the PHY and MAC software layers of the software stack, the ranging method should be adapted within the radio communications system and ideally operate in conjunction with data communication when possible. The localization method must also be adaptable to the upper layers of the software stack (typically the Zigbee stack).

The layers of IEEE 802.15.4 and Zigbee are both standardized and established, current ranging methods within those standards have failed to demonstrated the level of ranging accuracy required for WSNs. In the 2.4 GHz band, low rate data transfer is performed at 250 kb/s to reduce power consumption. The accuracy of TOA estimates is limited by signal bandwidth and therefore using IEEE 802.15.4 for accurate TOA range estimation could take tens of seconds. System clock frequencies on sensor nodes are typically below 40 MHz, limiting the resolution to TOA range estimates to less than 7.5 m. In alternative TOA ranging systems, the resolution of range estimates is bound by the frequency of the signal correlators sampling period which is typically below 10 MHz. This is a problem because WSN require ranging resolution better than 0.3 m and therefore

timing resolution requirements of better than 1 ns.

At the time of this research, ranging systems measuring the signal TOA had demonstrated better performance than alternative ranging techniques. However, those are limited by the synchronization requirements and use of very large bandwidth signals. In this work, the use of narrow-band (signal bandwidth < 5 MHz) RF TOF ranging is considered for distance estimation in WSNs. It is expected that low power, low processing overheads and available IEEE 802.15.4 communications protocol can be used to meet the requirements of TOA ranging. Alternative TOF ranging schemes have used UWB signals to achieve sub-metre ranging resolution [13], however, those are limited in operational range (< 100 m) because of the FCC regulation on transmission power. Futhermore, it is expected that ranging accuracy below $\pm$ 1.0 m can be achieved through the use of narrow-band RF signals and 0.3 m resolution can be achieved by sub-clock time periods known as 'jitter measurement'. This approach is time dependent in comparison to alternative frequency dependent techniques that have be considered [17]. In addition, most communications radio modules in WSN applications use narrow-band radio modules. For this reason alone it is clear that the ability to perform accurate range estimation by TOA under this constraint is both beneficial and advantageous.

Chapter 3

Limitations of Ranging

There are four fundamental factors that limit the performance of TOA ranging. Those include measurement resolution, measurement accuracy, synchronization and the effects of the wireless channel. Measurement resolution of a TOA ranging system is typically the greatest limiting factor because it is linked to the detection rate or clock period of the receiving devices timer. The clock period of those timers is typically much lower than required to meet the resolution requirements of TOA ranging in WSN applications. In contrast, the accuracy of range estimates is limited by noise and interference from both the wireless propagation channel and the associated ranging system hardware. Those errors can be reduced by three fundamental system parameters including signal bandwidth, the signal-to-noise ratio (SNR) and ranging duration. The devices involved with the ranging process also need to be synchronized in order that the receiving device can determine the transmission and reception times of the ranging signal. There are two techniques to synchronize devices involved with ranging including one-way and two-way-time-transfer (TWTT) . Finally, TOA ranging estimation can suffer significantly from reflected signals arriving at the receiver at different time delays. This phenomenon is known as multipath propagation and is a challenging problem for narrow-band TOA ranging systems. In this chapter the limitations of TOA ranging are detailed from the perspective of narrow-band signals because those are currently used in most wireless sensor node hardware platforms. The limitations are summarized in order to conclude the limitations of the novel ranging system described in the proceeding chapter.

3.1 Measurement Resolution

Narrow-band communications systems such as IEEE 802.15.4 operate by the transmission and reception of analogue waveforms which consist of ordered sequences of binary bits. When the analogue waveform arrives at the receiver, it is sampled at discreet time intervals and then cross-correlated with a local copy of the expected sequence for its de-

tection. The receiver must sample the received waveform above the Nyquist frequency ($f_{sample} \geq 2B$), where B is the signal bandwidth in order to fully recover all the information content of the signal. For a narrow-band RF TOF measurement system, resolution is limited by this time quantization introduced by the sampling period of the receiver's signal correlator [17] because this is the shortest time period that can be detected. This is denoted by equation 3.1. R is the TOF ranging resolution [m], c is the speed of light [ms^{-1}] and T_s [s] is the sampling period of the receiver signal correlator.

$$\pm R = \frac{cT_s}{2} \tag{3.1}$$

Ranging resolution in the specified application of WSNs is typically required to be 0.3 m as explained in chapter 1, and therefore $T_s \leq$1 ns; this corresponds to a signal correlator sampling rate $F_s \geq$1 GHz. This is not ideal in low-power WSN hardware because of the increased power requirements of higher frequency oscillators ($I[A] = dQ/dt$, as $dt \rightarrow 0$, $I \rightarrow \infty$). Commercially available sensor node hardware such as the TI CC2430 is compliant with IEEE 802.15.4 and utilises a modulation scheme with chips transmitted at 2 Mchips/s. The TI CC2430 receiver performs signal correlation at 8 MHz (T_s = 125ns). Therefore the expected resolution of TOF estimates is in the order of 37.5 m as derived from equation 3.2. From equation 3.2, it is clear that the ranging resolution is much low than that required in WSN applications when the resolution is bound by the quantization introduced by the signal correlator.

$$\pm \Delta R = \frac{cT_s}{2} = \frac{(3x10^8) \cdot (125x10^{-9})}{2} = \pm 18.75m \tag{3.2}$$

Time quantization introduced by the signal correlator can be reduced by sampling at least twice the signal correlator bandwidth (B) resulting in a TOF time resolution of 1/2B [63, 64]. This is because transmitter-receiver clock drift and noise contribute random error to the TOA estimate time which have duration over two time estimation intervals (time bins) that correspond to a ranging distance resolution of c/2B. The random error is assumed normally distributed within the two time bin intervals and by averaging multiple TOA measurements and assuming a normal distribution, the variance in range estimates corresponds to equation 3.3, where n is the number of ranging transactions averaged. Time quantization using this method is bound by 1/2B. For an IEEE 802.15.4 compliant receiver, this corresponds to range estimate resolution 18.75 m one-way which still below the resolution and accuracy requirements of WSNs. Furthermore, the resolution is linked to the frequency of the timer clock (clock quantization).

$$\sigma_{TOA} = \frac{c \cdot F_s}{\sqrt{n}} \tag{3.3}$$

To alleviate the aforementioned problems, a novel time-dependent TOA ranging method

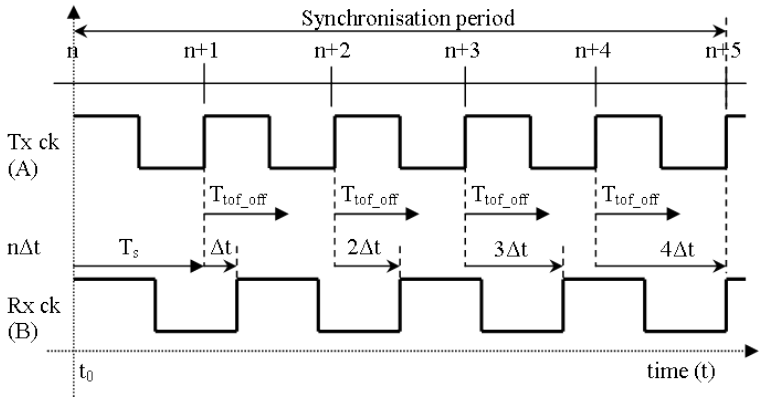


FIGURE 3.1: Time diagram to illustration of TOF sub-clock period phase measurement using correlator frequencies T_s and $(T_s + \Delta t)$ over successive range measurements. Transmit and receive assumed on rising clock edges.

is considered as an alternative to frequency-dependent methods. A sampling time period: $T_s \leq 1$ ns is achieved by considering ranging transactions between a transmitter and receiver with signal sampling periods T_s and $(T_s + \Delta t)$. The time difference Δt allows sub-clock phase offset measurement over multiple ranging transactions as shown in figure 3.1. Ranging transactions arriving at the receiver before T_{tof_off} have period τ and are binned in b_0. Ranging transactions arriving after T_{tof_off} have period $\tau + 1$ clock periods and are binned in b_1. T_{tof_off} corresponds to the sub-clock period or phase measurement of the TOA period. The number of ranging transactions n required to obtain the phase offset measurement is determined from $n = T_s/\Delta t$, and is defined herein as the synchronization period. The TOA period with phase offset measurement is finally extracted by finding the arithmetic mean as shown in equation 3.4.

$$\tau_{TOF} = \frac{1}{n}\sum_{i=1}^{n}(b_0 + b_1) \tag{3.4}$$

Ranging transactions are offset by one clock period for each measurement with the constraints $(0 < \Delta t \leq 0.5T_s)$ and Δt divisible by T_s in order to achieve TOA ranging with phase offset measurement. The Period Δt fundamentally limits the resolution of the TOA estimate similar to time quantization introduced with signal correlation in synchronized TOF ranging. The effects of noise, multipath signal propagation and frequency inaccuracies may be reduced by oversampling over the synchronization period (multiple ranging transactions over the synchronization period). Using this technique, TOA ranging estimates are time-dependent as opposed to the previous frequency-dependent methods. The phase measurement principle can be seen from the Vernier delay line [65], where in this implementation, the function of the two buffer delay lines is generated through the frequency difference Δt. The transmission time and period of the transmitter clocks are required at the receiver in order to recover the TOA period; this is achieved through synchronization detailed in the proceeding sections.

3.2 Measurement Accuracy

The accuracy of TOA ranging is bound by the random error introduced from both noise and interference. This is because noise and interference limit the receiver's ability to accurately distinguish the precise TOA of a ranging signal. Sources include but are not limited to thermal, shot and flicker noise. For example, thermally aggregated electrons in a conductor constitute a randomly varying current that gives rise to voltage. The 'available noise power' is the result and is defined by equation 3.5, where k[J/K] is Boltzmann's constant ($\approx$ 1.38 x 10^{-23}), T[K] is the temperature and B[Hz] is the noise bandwidth over which the measurement is made [66].

$$N_0 = N_0 B = kTB \tag{3.5}$$

Equation 3.5 shows that the total noise power depends on the measurement bandwidth assuming a constant ambient temperature. Using equation 3.5, it can be calculated that a communications link operating with a 2 MHz bandwidth (i.e. IEEE 802.15.4 communication link) has thermal noise 8.28 x 10^{-15} W (-111 dBm) at room temperature. This does not account for the additional contribution of thermal noise of the radio receiver which may also have a wider bandwidth than the channel. Hence, the design of the communications link including transmission power, signal modulation and transceiver analogue front end all contribute to the effect of noise. Thermal noise is consistent over any given absolute bandwidth (i.e. 1.000 GHz - 1.001 GHz or 2.400 GHz - 2.401 GHz) and is referred to as an additive white Gaussian noise (AWGN) source because of this consistency. The signal-to-noise ratio (SNR) is a common measure that relates the noise power P_0[w] to the average signal power P_s[w] within a communication link. More specifically, SNR can be expressed to relate energy per bit E_b[J], bit rate r[bits/sec], noise-power spectral density N_0 and bandwidth B[Hz] of the communication link as defined by equation 3.6.

$$SNR = \frac{P_s}{P_0} = \frac{E_b r}{N_0 B} \tag{3.6}$$

The performance of ranging is linked to the SNR in that the greater its value the more precisely the time-of-arrival period can be measured. This can be more easily understood by considering a simple rising-edge ranging signal arriving at an edge-detection receiver. When the rising-edge arrives, it may be detected slightly early or slightly late due to the noise added to the signal [63]. This early or late arrival is significant in TOA ranging because a delay of only 1 ns results in a range measurement error of 0.3 m. The rate of change of the rising-edge is proportional to the ranging signals bandwidth. The greater the bandwidth the faster the rise-time of the signal, thus the more accurate the ranging system. Furthermore, the noise amplitude increases as a root function of the bandwidth

and the signal transition speed increases linearly with bandwidth, therefore a ranging signal utilising greater bandwidth is more tolerant to noise [63]. To quantify those statements, a model is required which relates the limitation of ranging accuracy to the SNR and system bandwidth. This is derived using the Cramer-Rao lower bound for TOA estimates. The Cramer-Rao Bound (CRB) is an unbiased estimator for the lower bound variance of TOA range estimates defined by equation 3.7 [67], where the variance σ_{TOA} [m], is the TOA time error, B [Hz] is the spectral bandwidth of the ranging signal and SNR is the signal-to-noise ratio. It should be noted that a normalised SNR defines the energy per bit E_b over the noise power N_0 (E_b/N_0) and is commonly used to compare bit error rate (BER) performance of different digital modulation schemes without taking into account bandwidth.

$$\sigma_{TOA}^2 \geq \frac{1}{(2\pi B)^2 SNR}\left(1+\frac{1}{SNR}\right) \tag{3.7}$$

In most communication systems, the signal energy (E_s) is very much greater than the noise density (N_0). Therefore, the $(1+1/SNR)$ term contributes very little to the CRB lower bound estimate because $(1/SNR) \approx 0$. In addition, if n ranging transactions are performed as part of a TOA estimation, the variance the ranging decreases by a root function of the number of ranging samples. Therefore, the approximate CRB for n TOA ranging estimates is described by equation 3.8.

$$\sigma_{TOA}^2 \geq \frac{1}{4\pi^2 \cdot B^2 \cdot SNR \cdot n} \tag{3.8}$$

From equation 3.8 it can be seen that a quadratic improvement is made to the accuracy of TOA range estimates by linearly increasing the signal spectral bandwidth, hence why wide spectral bandwidth signals (i.e. UWB) are a good approach for accurate TOA ranging estimates. In contrast, only a linear improvement is made to TOA estimates by improving the SNR. The Cramer-rao lower bound range distance error d [m] is defined as the product $c \cdot \sigma_{TOA}$, where c is the speed of light [68]. Figure 3.2 shows Cramer-rao lower bounds on the ranging error for five different spectral signal bandwidths with n averaged samples. It can be seen that sub-metre ranging accuracy can be achieved by using a spectral bandwidth of as low as 2 MHz and averaging 3000 samples ($n = 3000$). In contrast, if signal spectral bandwidth can be increased, a quadratic gain is made. This is not always ideal because of the FCC regulation on transmission power using Ultra-wideband. Using less bandwidth and averaging greater numbers of ranging measurements is therefore a favourable approach. Time averaging has also been found to reduce the effects of multipath signal propagation and additive white Gaussian noise (AWGN) [68], the reason for this is explained in further detail in the proceeding section on multipath propagation. However, the use of multiple measurements increases the processing time which may introduce limitations on the estimation time and hence limit

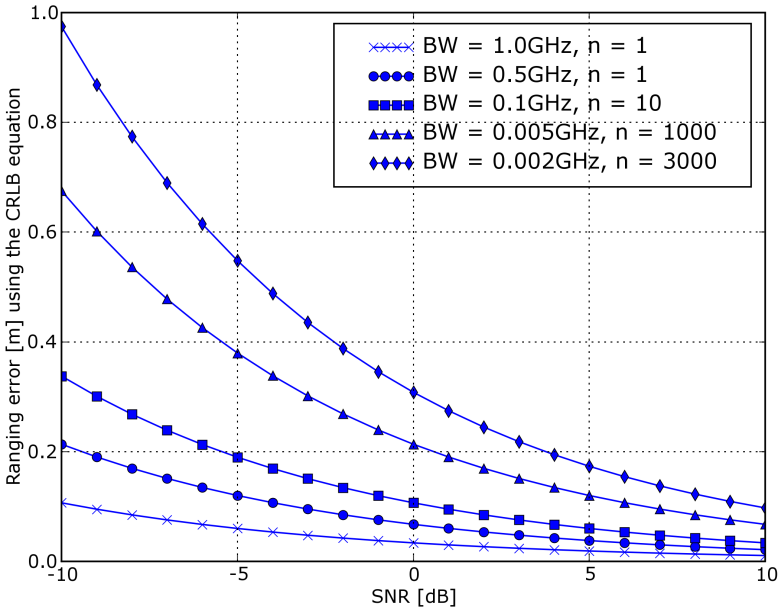


FIGURE 3.2: Cramer-Rao lower bound for TOF range estimates using different numbers of samples, bandwidths and signal-to-noise ratios.

the applications of the ranging scheme (i.e. make it unsuitable for real-time tracking systems). For those reasons, a trade-off must be made in the choices of system parameters including signal bandwidth, signal power, chip rate and ranging accuracy requirement.

The duration of a ranging signal also effects ranging accuracy by inspection of equations 3.6 and 3.8. The number of TOA range estimates made during each ranging signal made by the receiver is defined by the bit rate r in equation 3.6. From the perspective of the simple rising-edge detection scheme, all the useful range information exists in a very small time window and thus observing the signal for a longer period would not contribute to improving the accuracy of the range estimate. However, if multiple rising edges are detected and averaged by the receiver, this may be viewed as increasing the detection period or bit rate r and the accuracy of the range estimate is time-dependently improved [63]. Hence it is clear that using conventional narrow-band communications equipment, ranging accuracies comparable to wide-band systems can be achieved because of their longer signal transmission duration. Increasing the signals duration can be viewed as averaging multiple ranging signals and is also a good technique to reduce the effect of multipath [68], this will be discussed later. The bandwidth and duration of communications signals are linked such that $T_s B \approx 1$, where $T_s = 1/r$. By rearrangement of equation 3.6, the E_s/N_0 ratio is approximately equal to the SNR as shown in equation 3.9 [63].

$$\frac{E_s}{N_0} = T_s B \cdot SNR \tag{3.9}$$

Equation 3.9 indicates that if TOA ranging signals have large T_sB then they will have better noise immunity at low values of SNR. This is particularly attractive for narrow-band communications systems including IEEE 802.15.4 because DSSS is utilised to convert symbol sequences to 32-bit pseudorandom chip sequences with long duration. However, a disadvantage of long duration ranging codes ($T_sB > 1$) is the cost of increased signal processing time to estimate range. Using IEEE 802.15.4, this could fundamentally limit the possibility of being able to perform real-time tracking with the accuracy requirements of WSNs because of the additional latency involved with ranging. A trade-off must therefore be made between signal spectral bandwidth and the duration of signal detection in order to meet the requirements of the ranging system.

The CRB and SNR defined in equations 3.7 and 3.9 can be used to estimate the lower bound variance of TOA estimates using the IEEE 802.15.4 standard. IEEE 802.15.4 uses an offset quadrature phase shift keying (O-QPSK) modulation to modulate 32-chip sequences. The chip rate is 2 Mchip/s (bandwidth B) and it is assumed the typical SNR at the receiving device to be -20 dB (this will vary with range, typically between 0 dB - 30dB). Each 32-chip sequence corresponds to a symbol, where 1 symbol is 4-bits. IEEE 802.15.4 compliant packets have a preamble sequence of 4 bytes (excluding the SFD) for synchronization. By considering the use of a IEEE 802.15.4 packet for range estimation, the expected accuracy can be determined using the CRB. Equation 3.9 can then be used to calculate E_s/N_0 for a ranging packet with the aforementioned parameters, where the preamble is 4 bytes (8 symbol periods), each symbol has duration 32 us and the complete preamble lasts for 256 us (sum of I and Q phase duration) using an IEEE 802.15.4 compliant packet format.

$$\frac{E_s}{N_0} = T_s \cdot B \cdot SNR = (256x10^{-6}) \cdot (2x10^6) \cdot (0.01) = 5.12 \tag{3.10}$$

Substituting this into equation 3.7.

$$\sigma^2_{TOA} \geq \frac{1 \cdot c^2}{4\pi^2 \cdot (2x10^6)^2 \cdot 5.12} = (10.55m)^2 \tag{3.11}$$

This indicates that the lower bound accuracy for a single two-way range estimate using IEEE 802.15.4 is 10.55 m. It should also be noted that the modulation techniques also effects the accuracy of range estimates because of the chip shaping, however because the SNR is generally very large in short range communications applications, the impact of the modulation scheme on ranging performance is very small and therefore the CRB is a good approximator on the accuracy. Accuracy can also be improved by increasing the duration of the pseudorandom preamble sequence at the start of the ranging packet or by averaging greater numbers of ranging transactions. Ranging greater numbers of ranging transactions does however increases processing time and the improvement to ranging performance has a root function with the number of averaged samples (i.e. $\sigma_{TOA} =$

$1/\sqrt{n}$). In WSN applications, the narrow-band communication links used generally have very large SNR values. Therefore equation 3.9 states that E_b/N_0 is also very large. High values of E_b/N_0 allow the CRB to be nearly achieved in many systems, but the CRB is not a tight bound at low E_b/N_0 [63]. The accuracy of range estimates is also effected by multipath which is explained in the next section. Signal multipath is a difficult problem for ranging systems because it can interfere both positively and negatively on the performance of range estimates and is difficult to mitigate. IEEE 802.15.4 radios use a 2 MHz bandwidth and DSSS to reduce the effects of multipath, however, those narrow-band radio modules can suffer in high-multipath environments. One solution is to frequency-hop and perform ranging on different channels to increase the overall effective bandwidth of the channel to those effects. This is because different materials have different frequency responses, therefore by changing the carrier frequency different TOA estimates may be obtained. By averaging over multiple estimates on different carrier frequencies the accuracy of a range estimate may be improved. The alternative approve is to use wide-band ranging signals where a quadratic improvement in accuracy is achieved by linearly increasing signal spectral bandwidth as illustrated by equation 3.7. For this reason alone, a significant amount of research has been carried out on the development of UWB ranging and locating systems. UWB communications technology was originally referred to as base-band pulse, carrier-free or impulse communications systems reflecting that the transmission signal was wide-band with extreme rise-time or edge detection [69]. An UWB signal is defined by the Federal Communications Commission (FCC) and International Telecommunications Union Radio communication Sector (ITU-R) to be a signal that has bandwidth $\geq$500 MHz or occupies 20% of the centre frequency. Because of the significantly large use of bandwidth, UWB systems are restricted for use within the 3.1 GHz - 10.6 GHz spectral frequency band with maximum power spectral density (PSD) -41.3 dB/MHz. This is significantly low in comparison to narrow-band radios which typically have spectral transmission powers of -25 dB. UWB systems therefore have SNR limiting data throughput with increasing transmitter-receiver distance. Figure 3.2 illustrates the performance of UWB based systems for two-way ranging.

This section has shown that the accuracy of ranging is bound by two fundamental factors, the bandwidth of the ranging signal and the SNR or (E_s/N_0) value. The CRB lower bound variance is illustrated for different bandwidths and SNR values in figure 3.2 and it can be seen that sub-metre ranging accuracy is obtainable using narrow-band signals (bandwidth of 2 MHz). Alternately, UWB ranging systems can achieve precise range accuracy ($<$ 3.0 m) at the cost of reduced transmission power (i.e. regulation). In essence, the greater the bandwidth of the ranging signal, the lower the SNR, limiting the performance of those systems at larger transmitter-receiver distances. Therefore the bandwidth and SNR must be chosen to suit the application in question and meet the regulations within the communications bands. The focus in this work involves ranging between sensor nodes in compliance with the IEEE 802.15.4 standard which operates us-

ing narrow-band signals. Narrow-band signals are also widely used in a number of other subsequent standards where they have demonstrated excellent performance [29, 49]. Further techniques have been developed to provide resilience to noise and interference in those narrow-band systems. For this reason, the ability to determine range using narrow-band is important because narrow-band systems will be used for many years to come. The most widely used standard for communication in WSN applications is IEEE 802.15.4 which uses signals with 2 MHz bandwidth. This standard relies on detecting a received signals power for range estimation with the RSSI result filtered and converted to a linear distance-estimate relationship. As discussed in chapter 2, this technique of ranging is known to suffer from the effects of shadowing, scattering and interference presented by the wireless channel and requires complex models to account for those errors. Those complex models are not ideal for WSNs where hardware and power constraints make processing a difficult and costly task. It is also important to note, the CRB shows that sub-metre ranging estimates are obtainable through the use of IEEE 802.15.4 and multiple ranging transactions. In WSNs, transmitter-receiver distances are expected in the range of 0.0 m - 100.0 m and very large SNR values dependent on environmental factors in the range of 10 dB to 30 dB.

3.3 Synchronization

There are two constraints relevant to the determination of TOF measurements: (1) the transmitting (Tx) and receiving (Rx) devices must be precisely synchronized to a common system clock (ck) and (2) the receiving device must be provided with the transmission time of the ranging signal. From this perspective, a signal is transmitted from some device A at a known time ($t_{A-transmit}$) and is detected at a measured time ($t_{A\rightarrow B}$) with reference to a common system time. The range estimate can then be extracted by subtracting the receive time from the transmit time and multiplying this by the speed of the signals propagation. Synchronization of the Tx and Rx devices is a critical aspect on the accuracy of TOF estimates. An error in time synchronization of 10 ns would result in a range estimate error of 3 m (distance $= c \cdot t$). Therefore, synchronization tolerance of device clocks must be precise in order that the Tx and Rx remain synchronized for the duration of the ranging process. Synchronization is challenging in the application of WSNs because sensor nodes are not equipt with highly accurate and precise system clocks and equipting sensor nodes with clocks of this nature would be both uneconomic and impractical with respect to the power requirements and hardware overheads. The crystal oscillator clocks employed on sensor nodes have operating frequencies in the order of 1 kHz - 40 MHz with threshold accuracies of around $\pm$ 40 ppm. The frequency of those crystal oscillators are effected by temperature and supply voltage change [55]. For example, the TI CC2430 operates from a 32 MHz crystal oscillator which has a $\pm$ 40 ppm oscillation accuracy. Assuming two TI CC2430s

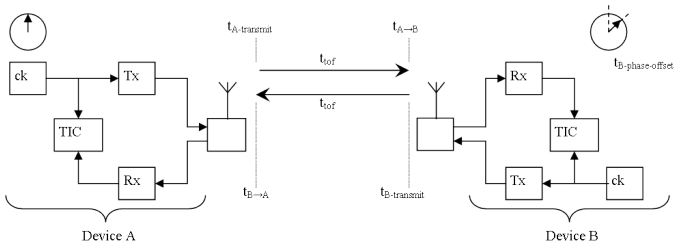


FIGURE 3.3: Two-way time transfer technique for TOF device synchronization [70].

are involved with a TOF ranging process and a 20 ppm frequency difference exists between the devices, for a range distance of 30 m (TOF = 0.1 us), this implies the TOF estimate error would be 2 ps ((0.1us/1x10^6)x 20 ppm), a resultant range estimate error of 0.3 mm. This is a small estimate error and does not account for the transmit, receive and processing delays of the TOF measurement system. However, this example assumes that the device clocks are synchronized at the start of the TOF measurement process but does not detail how this can be achieved. If the same TOF ranging process was performed several seconds after this synchronization time, the range estimate error would be significantly larger. There are two methods of synchronizing the devices A and B categorised as one-way transaction and two-way-time-transfer (TWTT). Using one-way transaction, synchronization between the Tx and Rx is achieved by the use of different signal frequencies. An electromagnetic signal is used to synchronize the devices and a slower acoustic signal is used to measure the TOF [45]. This approach is not ideal in WSNs because Ultrasonic transducers are bulky and consume additional power. In contrast, TWTT technique [70] is illustrated in figure 3.3 where devices A and B incorporate transceivers as opposed to a single transmitter and receiver. The method is used to compare two clocks or oscillators in order to reduce the phase offset (in clock cycles) and hence synchronize the devices. A and B operate from independent system times which are unsynchronized and have some phase offset where the resolution of the technique is bound by the period of the clock at device A. The phase offset and signal TOF between A and B are derived from equations (3.12 to 3.15), where ($t_{A-transmit}$) and ($t_{B-transmit}$) are the transmit times, ($t_{A\rightarrow B}$) and ($t_{B\rightarrow A}$) are the received times, (t_{tof}) is the time-of-flight period and ($t_{B-offset}$) is the phase offset of device B's clock with respect to device A's clock. The unsynchronized two-way time transfer measurements include the phase offset as an additive term in the forward transfer and a subtractive term in the reverse transfer with respect to A's clock. The additive phase offset can be removed by averaging multiple two-way transfers and hence a more accurate TOF period is obtained. The TOF period is extracted from the time interval counter (TIC) or free-running timer. This is then calibrated to correspond to the true distance d[AB] by using $d[m] = \tau c$, where c is the speed of light (3 x 10^8ms^{-1}).

$$t_{A\to B} = t_{A-transmit} + t_{TOF} + t_{B-offset} \tag{3.12}$$

$$t_{B\to A} = t_{B-transmit} + t_{TOF} - t_{B-offset} \tag{3.13}$$

$$t_{TOF} = \frac{1}{2}[(t_{A\to B} + t_{B\to A}) - (t_{A-transmit} + t_{B-transmit})] \tag{3.14}$$

$$t_{offset} = \frac{1}{2}[(t_{A\to B} - t_{B\to A}) - (t_{A-transmit} - t_{B-transmit})] \tag{3.15}$$

Achieving the precise levels of synchronization ($<$ 1 ns) for either one-way or TWTT techniques in WSNs is a difficult task. This is because precise, highly accurate clocks are expensive and an impractical solution for resource constrained, inexpensive sensor nodes which operate from inaccurate crystal oscillators. Alternative systems have utilised TDOA ranging with wired infrastructure to alleviate the problems associated with synchronization [22, 13]. For those reasons, two-way ranging with unsynchronized or relaxed synchronization device clocks at A and B is considered in this work. Device B simply waits for a ranging message to be received and returns this message after a known response delay. Therefore, device B requires no knowledge of the common time base or a time-stamped ranging message from device A. Device A simply measures the round-trip period which consists of two TOF periods, a clock phase offset and a response delay at the device B. The response delay at B is a fixed period and thus only the phase offset changes over time because of the inaccuracies of the device system clocks. In WSNs this would correspond to the small frequency difference Δt between the crystal oscillators at devices A and B. The period Δt is within the bounds ($0 \leq \Delta t \leq t_b$), where t_b corresponds to the time period of one clock cycle of device B's clock. Therefore the maximum range estimate error is $c \cdot t_b$ in the absence of noise and multipath. Two-way ranging is computationally more demanding in comparison to one-way ranging because of the requirements of transceiver, transmit-receive switching and TOF message turn-around processing. Two-way ranging also takes longer to execute because of the return message required to remove the synchronization overhead. Inconsistent time delays in the transceivers can also result in large range estimate errors. However, by considering the noise performance of two-way ranging which is found from the CRB for TOF range estimates, the noise performance of a two-way range measurement is the average of two one-way TOF measurements denoted by equation 3.16.

$$\sigma^2_{TOA} \geq \frac{1}{2(2\pi B)^2 \cdot SNR} \tag{3.16}$$

This indicates that two-way ranging has improved performance in the presence of noise. However this is at the cost of additional time for range estimation. In WSNs this is not a problem because standards such as IEEE 802.15.4 could combine two-way ranging with data packets. The receiving device would measure the time period in clock cycles

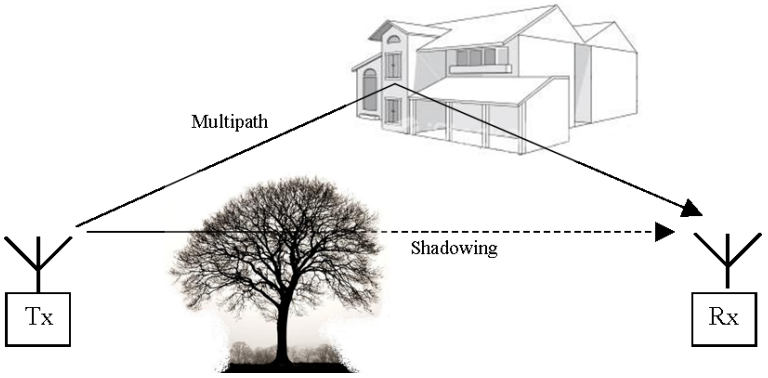


FIGURE 3.4: Wireless channel multipath and shadowing examples.

of data reception. Following this process, the receiving device would transmit an *acknowledgement* packet back to the device A in order that device A can determine the round-trip period and hence the range between devices A and B.

3.4 Wireless Channel Effects

When a ranging signal propagates through the wireless channel, it may encounter obstacles with surfaces which reflect or diffract the signal. In addition, obstructing obstacles within the direct transmitter-receiver path may cause excess attenuation of the direct-path signal. The phenomena of reflected or diffracted replicas of the direct path signal are known as Multipath. Attenuation of the direct-path signal resulting from obstructing obstacles is known as Shadowing [18]. In some circumstances, such as indoor environments, multipath and shadowing can contribute the dominant error in range estimates. Figure 3.4 illustrates typical examples of multipath and shadowing where T_x is a transmitting device and R_x is a receiving device. In case of shadowing, the ranging signal must propagate through an obstructing tree causing a large attenuation result to the signal. For the case of multipath, the signal received at the receiver has been reflected off the surface of a building. It is clear from figure 3.4 that multipath and shadowing are a result of the environment. The amplitude and phase of a ranging signal are effected by both multipath and shadowing. However, shadowing alone does not effect TOA range estimates because the direct path is always the first arrival at the receiver and thus it is the ability of the receiver to detect this first arrival that limits the performance of range estimates. In a multipath environment, the receiver must determine the direct path range estimate or first arrival and ignore the other paths else range estimates become errored by the multipath components [63]. For example, if the receiver is only able to track a multipath signal due to obstructions in the direct path, this will result in an inaccurate range estimate. In contrast, shadowing only exists over a distance proportional to the length of the obstruction and is thus a small error contribution in comparison to that of the channel path-loss.

Reflected signals have longer paths than direct signals and are therefore delayed. The time difference in propagation (T_{delay}) along two signal paths (i.e. direct and reflected path) is known as the *delay spread* defined as $T_{delay} = (t_{reflected} - t_{direct})/c$. The direct-path signal can easily be determined by a receiver in the presence of multipath if T_{delay} is greater than twice the spreading code symbol period [18]. This is because the multipaths distort the correlation function between the received signal composite (direct plus multipath) signal and the local reference copy generated in the receiver. Thus, when T_{delay} is greater than twice the symbol period, provided the receiver can track the direct-path signal, multipath has little or no effect on ranging estimates. However, for an IEEE 802.15.4 compliant radio receiver which receives symbols of duration 16 us (32 chips at 0.5 us/chip), it is clear that at short range, those narrow-band radios are effected by multipath which can interfere constructively or deconstructively with range estimates. IEEE 802.15.4 compliant radio modules operating at 2.4 GHz ($\lambda = 0.12$ m at 2.4 GHz) can suffer significantly from multipath because moving the transmitter and receiver only a small distance apart significantly changes the receivers view of the multipath. Thus, how the channel changes is linked to the relative motion of the transmitter and receiver. Multipath interference is also dependent on the power and phase of the multipath signals relative to the direct-path signal. Multipath signals with significantly less power than the direct-path signal do not dramatically affect the performance of range estimates.

It is sometimes useful to describe multipath in terms of a simple model in order to understand its effect more easily. The simplified multipath model describes a set of independently reflected signals with different amplitudes and phase offsets which are delayed in time with respect to the direct-path. A signal $s(t)$ in the absence of multipath is described in complex notation by equation 3.17, where $x(t)$ is the complex envelope of the transmitted signal, τ is the time for the signal to propagate from the transmitter to receiver and f_c is the carrier frequency.

$$s(t) = \alpha_0 x(t-\tau) e^{-j\phi_0} e^{j2\pi f_c (t-\tau)} \tag{3.17}$$

When multipath signal propagation exists, the complex envelope of the received signal $r(t)$ in the absence of noise and interference and following frequency down conversion is represented by equation 3.18. There are N multipaths, α_0 is the received amplitude of the direct path and the α_n are the received amplitudes of the multipath returns, τ is the propagation delay of the direct path, τ_n is the propagation delay of the multipath returns, ϕ_0 is the received carrier phase of the direct path, ϕ_n is the receiver carrier phase of the multipath returns and f_n is the received frequencies of the multipath returns relative to the carrier frequency.

$$r(t) = \alpha_0 e^{-j\phi_0} x(t-\tau) e^{-j2\pi f_c \tau} + \sum_{n=1}^{N} \alpha_n e^{-j\phi_n} x(t-\tau_n) e^{j2\pi f_n t} \tag{3.18}$$

The parameters in equation 3.18 are generally time-variant because the motion of the receiver as well as the obstructions that cause the multipath surroundings relative to the transmitter-receiver direct-path change over time in many communications systems (i.e. tagged device relative to a set of reference transmitters). For this reason, equation 3.19 is a better representation for the time variant channel using parameters that relate the multipaths to the direct path.

$$r(t) = \alpha_0 e^{-j\tilde{\phi}_0} \left[x(t-\tau) + \sum_{n=1}^{N} \tilde{\alpha}_n e^{-j\tilde{\phi}_n} x(t-\tau-\tilde{\tau}_n) \right] \tag{3.19}$$

where $\tilde{\alpha}_n = \alpha_n/\alpha_0$ is the multipath-to-direct ratio (MDR) of amplitudes, $\tilde{\tau}_n = \tau_n - \tau$ is the excess delay of the multipath returns and $\tilde{\phi}_n$ are the received carrier phases of the different signal components. The multipath profile producing equation 3.19 can be portrayed graphically as a power-delay profile (PDP) by plotting the points $(\tilde{\tau}_n, \tilde{\alpha}_n^2)_{n=1}^{N}$ [18]. This model assumes that both the multipath components and the direct-path component have equal carrier frequencies, thus is not suitable when multipath signals arrive at different doppler shifts with respect to the direct signal path (i.e. receiver is in motion). Equation 3.19 with N=1 and time-invariant parameters is widely used in theoretical assessments of multipath performance due to its ease of use. However, the one-path specular multipath model provides the limiting case of zero doppler spread (time-invariant impulse response) and infinite delay spread.

For the aforementioned reason, equation 3.19 has limited realism for modelling the effects of multipath in the real-world and therefore more generalized methods are used. Ray-tracing is a technique used to approximate the propagation of an electromagnetic wave in the presence of multipath assuming a finite number of reflectors with known positions and dielectric properties. There are many variations of the ray-tracing model; one of the simplest is for the signal variation resulting from a ground reflection interfering with the LOS path. In contrast, complex ray-tracing models aim to predict signal propagation for more generalized propagation environments. Ray-tracing enables the effects of channel attenuation, reflection, diffraction, scattering and multipath components of a propagating signal to be approximated and modelled with simple geometric equations. It has been shown that when ray-tracing is compared with empherical data, the model can accurately determine the received signal power in rural, urban and indoor environments [18]. Examples of computer software for ray-tracing indoor and outdoor environments include Lucent's wireless systems engineering software (WiSE) [71] and Wireless Global Technologies CelPlanner Suite [72]. However, many models are developed for specifically for recorded data, frequency ranges and geographical environments and are therefore considered impractical for the general case.

One of the simpler and more practical representations of a wireless channels complex terrestrial multipath is shown in figure 3.5. This representation is based on equation 3.18

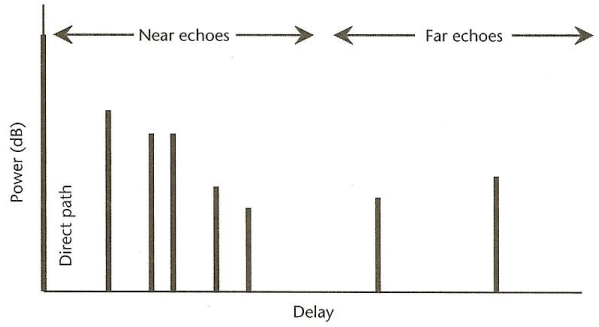


FIGURE 3.5: Canonical power delay profile representation for multipath signal arrivals at a receiver after transmission over a wireless channel [18].

where the signal arrivals are grouped as the direct path, discreet near and far echoes. The mean received power of echoes decreases exponentially with delay and there are typically many less far echoes than near echoes. The number of near and far echoes are each Poisson distributed, described by different Poisson parameters. Multipath phases are modelled as independent and identically distributed over 2π radians, where tables of statistical parameters for these components are provided for many different environments (e.g. open, rural, urban, motorway) and elevations [18].

The aforementioned models do not account for the fact that the transfer function of a channel at a given frequency varies over time and therefore the time variation of the wireless channel must be defined. This time variation is described by the correlation of transfer functions at different times using the same signal carrier frequency. In simple terms, if this variation in the channel is faster than the detection rate of the receiver tracking loops, multipath errors are smoothed by the receiver processing algorithms. In contrast, if the variation in the channel is slower, the multipath errors produce a time-invariant error term. The power spectral density (PSD) resulting from the Fourier transform of this correlation is called the doppler power spectrum of the channel and the range of frequencies over which it is essentially nonzero is called the channel *doppler spread* [18]. Dopper spread D_s [Hz] is represented by equation 3.20, where c is the speed of light, f_c [Hz] is the carrier frequency and v is the velocity of the receiver with respect to the transmitter.

$$D_s[Hz] = \frac{f_c v}{c} - \left(-\frac{f_c v}{c}\right) = \frac{2 f_c v}{c} \tag{3.20}$$

The time over which multipath can be regarded time-invariant is known as the *coherence time* (T_c) of the channel. It is the time over which a signal does not change appreciably. By applying the relationship $t = 1/f_c$, the coherence time is described by equation 3.21. By applying the relationship $\lambda = c/f_c$, then the coherence time corresponds to the time period of half a carrier signal wavelength or the time to travel from peak-to-valley denoted by equation 3.22.

$$T_c[sec] = \frac{c}{2f_c v} \tag{3.21}$$

$$T_c[sec] = \frac{\lambda}{2v} \tag{3.22}$$

Equation 3.22 indicates that if the range measurement period is less than T_c, the channel can be regarded as time-invariant even in the presence of multipath and receiver motion. Doppler spread is often dominated by the motion of the receiver with respect to the transmitter. The corresponding coherence periods range from milliseconds for stationary receivers or multipaths with large excess delays and tens of milliseconds for receivers in motion or multipaths with small excess delays. To quantify this statement, consider an IEEE 802.15.4 radio which operates on a 2.4 GHz carrier frequency. The receiver may typically have motion of 1 ms^{-1} when attached to a person walking or 13.41 ms^{-1} if attached to a vehicle travelling at 30 mph. The corresponding coherence times using equation 3.21 are calculated in equations 3.23 and 3.24.

$$T_{c(1ms^{-1})} = \frac{c}{2f_c v_{1ms^{-1}}} = \frac{3x10^8}{2(2.4x10^9)1} = 62.5ms \tag{3.23}$$

$$T_{c(13.41ms^{-1})} = \frac{c}{2f_c v_{13.41ms^{-1}}} = \frac{3x18^8}{2(2.4x10^9)13.41} = 4.66ms \tag{3.24}$$

Those are the maximum time periods that a range estimate must be performed within in order to mitigate the effects of multipath because of the time-invariant channel using IEEE 802.15.4. Two important factors can be noted from this derivation in order to mitigate or reduce the effects of multipath: 1) reducing the period of time required to perform a range estimate (i.e. try to make time period less than T_c) such that the channel remains time-invariant; 2) use a range of measurement frequencies together (i.e. UWB) since this interference effect is closely linked to carrier wavelength. It is reported that altering the carrier frequency by as little as 1% can dramatically change the apparent multipath environment in narrow band systems [63] and thus the ability for the receiver to identify the direct-path signal in the presence of multipath is linked to the bandwidth of the signal. Inter-path delays $t\delta p$ separate by more than 1/b in time are resolvable and paths separated by 1 m or more, a bandwidth of at least 300 MHz is required, showing a significant advantage of UWB based ranging systems [63]. Techniques that utilise larger signal bandwidth synthesisers from one or more narrowband signals are known as *super resolution* ranging methods and attempt to produce range resolution better than $1/b$ [63]. Multipath can also be mitigated through signal processing techniques categorised by parametric and nonparametric processing. Parametric processing aims to estimate parameters associated with the multipath in order to correct for their error in the direct path TOA estimation. In contrast, nonparametric processing employs

discriminator designs that are less sensitive to multipath-induced errors. Alternative methods to mitigate the effects of multipath include smart antennas such as the Choke ring that attenuate multipath reflections, particularly multipaths that arrive at elevation angles above or below the expected arrival path. However, this technique is more closely linked to AOA ranging because of the directional placement of antennas.

In WSNs, ranging is used to determine the position of a blind device in relation to a number of independent references with known positions. Each range estimate will encounter independent multipath effects and thus the resulting estimate errors are also independent. Multipath environments are challenging to model, they are both complicated and diverse because multipath and shadowing are both highly variable. It is therefore difficult to quantify the effects of those errors in both an accurate and general way. For example, the contribution of multipath for a transmitter and receiver with a direct LOS path is much less than for the case where the direct path passes through walls or foliage. One of the simplest multipath mitigation techniques is through the placement of those references (i.e. at least three available in each room for indoor environment). Computer simulations that synthesize waveforms and then employ high-fidelity channel models and specific receiver processing approaches to assess multipath can provide accurate and realistic numerical assessments, however those are often not representative of the real-world multipath conditions and provide limited insight into the underlying issues and characteristics.

3.5 Discussion

In this chapter, the limitations of ranging estimates for a given system with limited bandwidth, transceiver sampling period and synchronization threshold have been discussed. The focus of this research is on the problem of accurately and reliably determining range in WSNs for the purpose of determining position of sensor nodes with respect to some fixed co-ordinate system. Those sensor nodes have limited processing resources and energy conservation is an important issue to maintain the life expectancy of the WSN. For those reasons, this work focuses on developing a TOF ranging method which is adaptable to current wireless standards such as IEEE 802.15.4 and does not require additional hardware overheads which consume additional power and increase the duty cycle of sensor nodes during a localization process within a WSN. To conclude the limiting factors of range estimates they can be considered from the size of error they induce in the ranging system. In alternative narrow-band ranging systems [26], the resolution of range estimates is limited by the sampling rate of the signal correlator. This is the largest limit in range estimation since frequencies in excess of 300 MHz are required to achieve sub-metre ranging resolution. To mitigate this quantization problem, a novel approach of using frequency difference between transceivers is considered herein. This is explained in detail in the next chapter. The accuracy of those TOA range estimation is

limited by the signal bandwidth and SNR. Equation 3.7 illustrates that a quadratic improvement can be made to the performance of TOA estimates by linearly increasing the signal bandwidth. UWB ranging systems have demonstrated their ability to estimate range to very high accuracy and resolution, however, the use of wideband signals limits their practical operating range in comparison to narrow-band system. In addition, this is outside the limitations of narrow-band radios which are typically used in WSNs. In addition, figure 3.2 illustrates that time-averaging over multiple TOA range estimates can be used to improve a TOA estimate using narrow-band signals. This is particularly adaptable in standards such as IEEE 802.15.4 since range estimates can be performed simultaneously with data communications, thus mitigating the use of additional channel bandwidth for range estimation. Multipath and shadowing are both significant problems for narrow-band communications systems. However, narrow-band systems have demonstrated excellent performance in multipath environments despite this argument. Multipath and shadowing error mitigation techniques for narrow-band systems have been considered in the literature [64, 73, 74] and it is expected that further development of those algorithms and implementation to narrow-band systems could significantly reduce the effects of multipath and shadowing. However, in some circumstances such as complex indoor environments, solving for the direct TOA signal path is not possible using any technique of multipath mitigation, for example ranging through walls. The resulting range estimate will therefore be highly inaccurate and thus the use of referencing architecture and complex position estimation algorithms can be used to mitigate this error. Techniques to mitigate the effects of multipath and shadowing are considered outside the scope of this research and have therefore only been summarized herein. To meet the constraints of WSNs, narrow-band radios remain the most beneficial approach for date communication, range estimation and energy efficiency. For those reasons, the ability to perform TOA range estimates with high resolution and accuracy within those constraints is fundamentally important.

Chapter 4

Prototype Ranging System

In chapter 3 the four key limitations on the performance of TOF range estimates are considered in order to meet the resolution and accuracy requirements of the localization process of a WSN. In this chapter, a novel algorithm is prototyped and developed to enable the estimation of a point-to-point distance between two sensor nodes as part of the localization process. The design and development is carried out in four key stages by consideration of available hardware detailed in chapter 2 and ranging limitations detailed in chapter 3. Timing measurement, synchronization, system implementation and expected performance are considered in order to meet the resolution, accuracy and latency requirements of WSNs. Furthermore, compatibility with existing hardware and low power, low rate communications standards are addressed by development of the system using IEEE 802.15.4 communications protocol. A TI CC2430 development kit [33] has been selected for the design, prototyping and testing of the algorithm. The TI CC2430 is particularly suited for WSN applications and can be deployed for long periods when low-duty cycle software systems are employed. Details of this platform are outlined in chapter 2 and an in-depth reading can be found in [55]. Power consumption is not considered in detail for this ranging system because the algorithm could operate in conjunction with data packet transfer, thus contributing very little additional communication overheads in comparison to RSSI ranging currently employed in both the TI CC2431 and IEEE 802.15.4 standard. The prototyped algorithm operates entirely using the TI CC2430 single chip package. Software is produced in C, compiled using the IAR compiler and flash programmed onto the TI CC2430 development platforms using the Chipcon flash programmer. The resolution of range estimates are dependent on the frequency difference between the two sensor nodes involved with a ranging process. In comparison to alternative frequency dependent methods [17], this approach is time dependent meaning that the accuracy and resolution is improved over multiple TOF estimates. Ranging transactions are performed in the 2.4 GHz ISM band on a single channel and can be integral with data transfer in WSN applications. The algorithm may also be implemented in other communication schemes with similar hardware archi-

tecture and communications protocol. Hardware and software perspectives are detailed in this chapter for the prototype system.

4.1 Ranging Algorithm

It has previously been shown in chapter 3 that in order to improve the resolution of TOF measurements, the frequency of the synchronizing clock or signal correlator must be increased to reduce the sub-clock measurement period Δt illustrated in Figure 3.1. To achieve sub-metre ranging resolution by TOF measurement, a synchronizing or sampling frequency of greater than 300 MHz would be required to meet the 3.3 ns timing requirement. This is impractical for WSN applications because energy consumption and hardware are constrained in order to maintain the life of the network and reduce hardware costs of the sensor node. To mitigate this overhead, the principle of the Vernier Delay Line (VDL) [65] is utilised enabling a time dependent technique to reduce the phase offset Δt in TOA measurements and hence improve the time measurement resolution using low frequency timer clocks. Figure 4.1 illustrates the phase measurement scheme using a simple one-way TOF transaction between a transmitter A and receiver B which are both synchronized to a common system clock. The period t_d represents the phase offset which must be determined in order to improve TOA measurement resolution. For simplicity of explanation, a rising clock edge is used to describe TOA estimation which is assumed to be time stamped in order that the TOA period can be recovered at device B. The phase offset t_d can be determined by three techniques; using multiple signal detectors delayed in time on device B; by multiple TOA measurements delayed or advanced in time for each measurement; detection at device B delayed or advanced for successive TOA measurements. Multiple detectors at device B would be a costly overhead in terms of power consumption and physical size of hardware; and is therefore consider an impractical phase measurement solution. The solution of delaying/advancing the detection at device A or B over multiple TOA transactions is therefore considered to estimate the phase offset t_d.

To achieve the delay/advance of the detection time at device B (enabling device A to be 'system time'), the VDL digital structure illustrated in figure 4.2 is considered. Its function is used for on-chip phase measurements in high-speed computer and communications systems [75, 76, 65]. Phase measurement in this context is also sometimes refered to as 'jitter measurement'. The VDL structure consists of a serise of D-latchs and two delay line buffers. The lower delay line buffers are designed to be slightly shorter than those in the upper delay line by Δt [sec]. When two input rising edge signals clk_in and ref_clk are applied at the inputs, the phase offset of clk_in is measured with respect to the zero-phased reference clock ref_clk. As the clock edges propagate through each buffer stage, the phase difference between clk_in and ref_clk decreases by Δt [sec] and the D-latch outputs up to this stage are logic high. When Δt reaches zero, proceeding

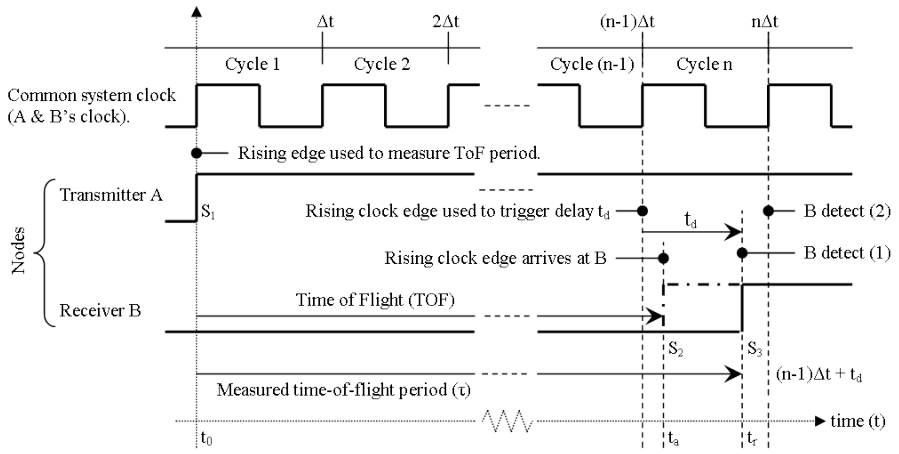


FIGURE 4.1: Timing diagram of synchronized TOF ranging between a transmitter A and receiver B using a common system clock. Phase offset t_d must be determined to improve TOF ranging resolution.

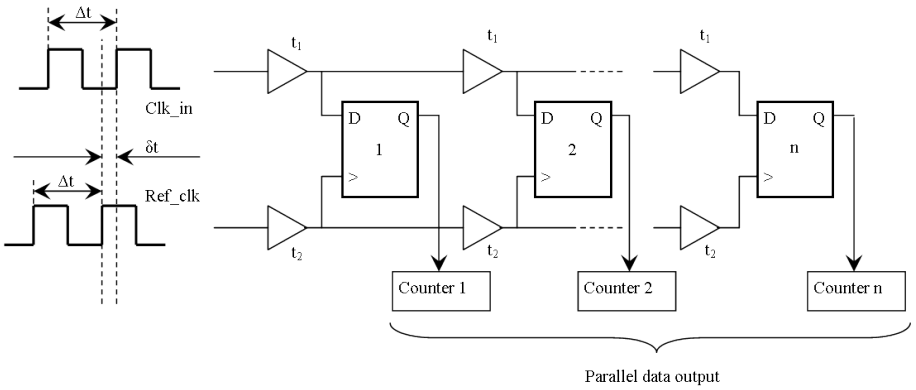


FIGURE 4.2: Vernier delay line schematic diagram [65].

D-latch outputs remain low and hence phase measurement is recorded by the output states of the D-latches. Over multiple executions of this process, the phase cumulative distribution function (CDF) and corresponding RMS phase value can be obtained by recording the logic state of each D-latch output using counters. Phase measurement resolution is reported to as low as tens of pico-seconds [65] using the VDL, where the measurement resolution is dependent on the number of buffer stages and the difference between t_1 and t_2 (Δt).

To implement the principle of the VDL in a TOA ranging system, its function is considered from the frequency perspective. The delay buffers perform the function of triggering the D and trigger inputs of a single D-latch at two frequencies ($f_1 = \frac{1}{t_1}, f_2 = \frac{1}{t_2}$) with difference $\Delta t = |t_{ref\_clk} - t_{clk\_in}|$ as shown in figure 4.3. Assuming clk_in and ref_clk begin in-phase, then each trigger clock edge of clk_in signal is shifted in time by $n\Delta t$ with respect to ref_clk, where n is the n^{th} cycle of ref_clk signal following t_0. The serial logical data stream is provided at the D-latch output for each shifted phase measurement. Any phase offset δt which exists between ref_clk and clk_in is determined either

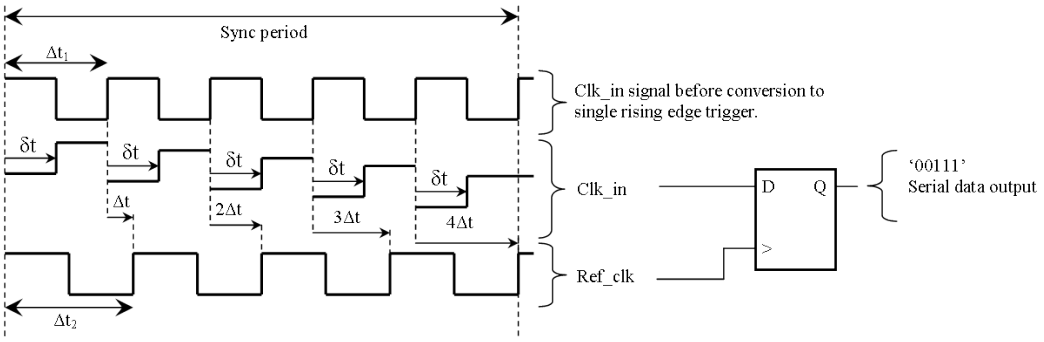


FIGURE 4.3: Vernier delay line principle using different frequency inputs.

TABLE 4.1: Table (Relationships between sync, Δt, ref_clk and clk_in.)

	SYNC clock cycles	SYNC time period
if $clk\_in > ref\_clk$	$n_{clk\_in} = \frac{ref\_clk}{\Delta t}$	$t_{sync} = n_{ref\_clk}.t_{clk\_in}$
if $ref\_clk > clk\_in$	$n_{ref\_clk} = \frac{clk\_in}{\Delta t}$	$t_{sync} = n_{clk\_in}.t_{ref\_clk}$

by the transition in state of the serial output bits or by averaging the serial data stream over the synchronization period. The phase measurement resolution Δt is decided by the frequency difference between clk_in and ref_clk. To explain the operation of the VDL shown in figure 4.3, timing diagrams are provided in figures 4.4 and 4.5 for the cases where $f_{clk\_in} > f_{ref\_clk}$ and $f_{clk\_in} < f_{ref\_clk}$. It is assumed for simplicity of explaination that the D-latch is ideal, the frequency of ref_clk is less than the input signal clk_in and clk_in is phase shifted by δt with respect to ref_clk when the signals are in phase. The synchronization (sync) period is defined to be the number of clock periods of the lower frequency that the signals are out of phase, hence clk_in and ref_clk are choosen to have difference in period Δt. Table 4.1 summarizes the relationship between all system parameters, where, Δt is the phase measurement resolution, t_{clk_in} and t_{ref_clk} are the periods of the input signals respectively, t_{sync} is the synchronization period and n_{clk_in}, n_{ref_clk} are the number of clock periods clk_in and ref_clk are out of phase. To avoid aliasing of the output serial data stream, only a single trigger input (clk_in) can occur over the duration of each sync period. Hence the system is time dependent and n_{clk_in} or n_{ref_clk} executions of the TOA estimations must be performed to achieve a single TOA estimate with phase offset measurement.

In figure 4.4, clk_in signal is phase shifted by t_d with respect to ref_clk and the synchronization period is chosen to be four clock periods for the simplicity of illustration. At time t_0, the D-latch is triggered by ref_clk. Since clk_in is in a zero state, the Q output of the D-latch registers as zero. The Q output does not change even if clk_in changes state and a reset must be performed before the next measurement. In this example, the next phase measurement is performed after six clock periods, i.e. in the next sync

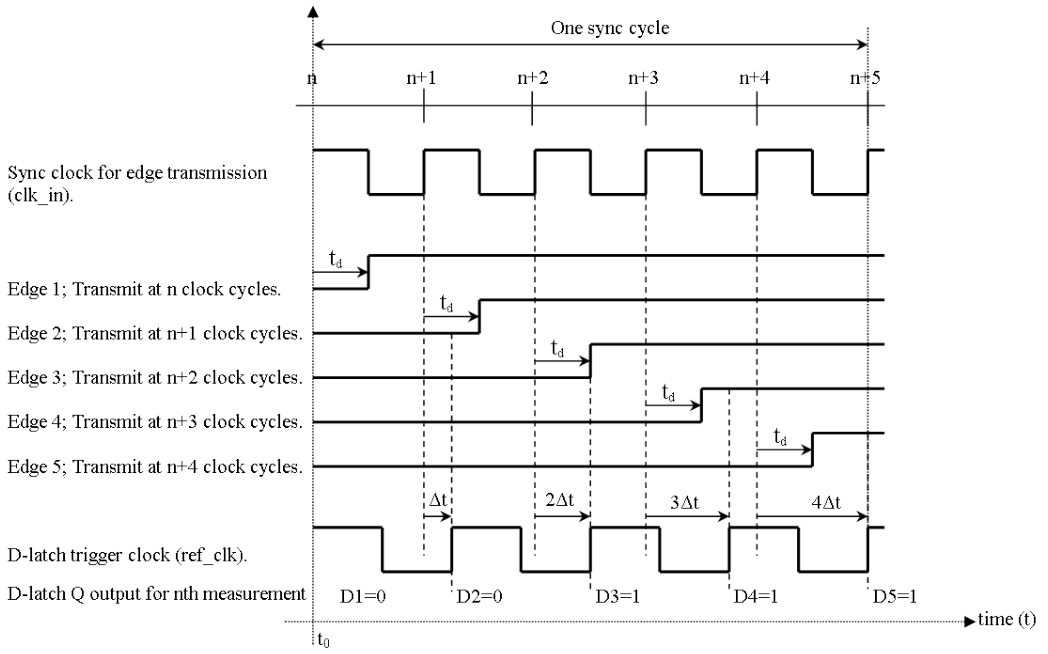


FIGURE 4.4: Timing diagram for Vernier delay line principle using different frequency inputs with frequency clk_in greater than frequency ref_clk.

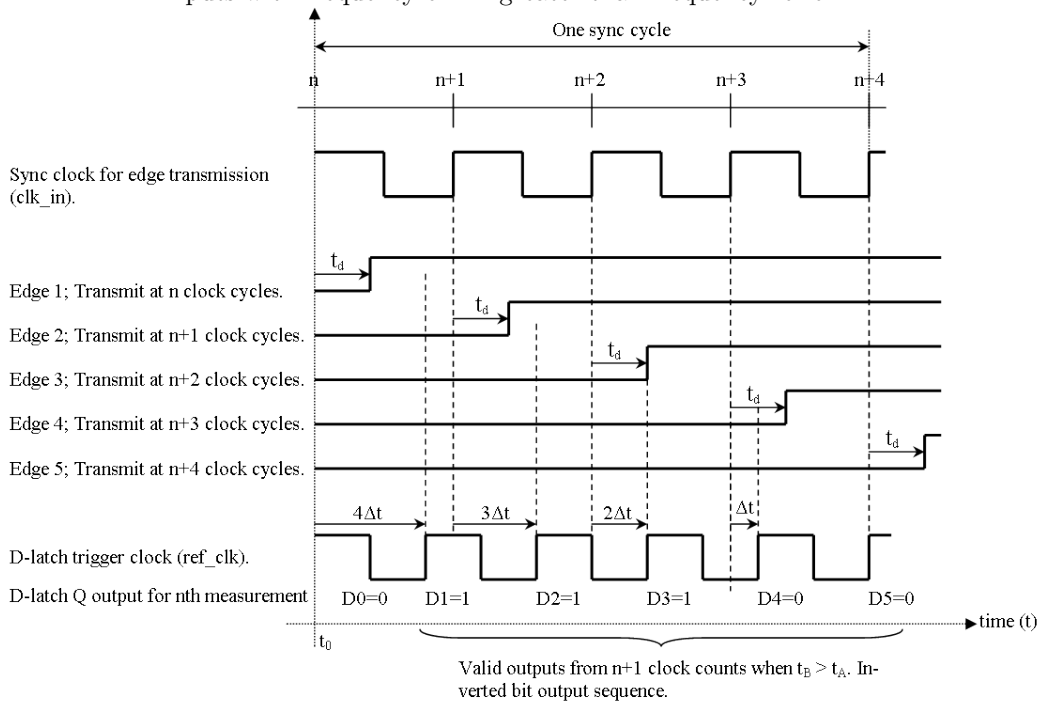


FIGURE 4.5: Timing diagram for Vernier delay line principle using different frequency inputs with frequency clk_in less than frequency ref_clk.

period to avoid aliasing the serial data output. The D-latch is reset and triggered on the $(n+1)^{th}$ clock cycle of ref_clk signal. At this point, ref_clk has caught up with clk_in by Δt, but clk_in is still logic low and hence the corresponding output state of the D-latch is logic low. For each phase measurement, ref_clk catches up with clk_in by Δt and the corresponding state of clk_in signal is latched on to the output of the D-latch.

In figure 4.4, the trigger edge clk_in+t_d and ref_clk are in phase after the n+2 clock cycle since the phase offset time period t_d is greater than $2\Delta t$ but less than $3\Delta t$. The transition of the D-latch output state from zero to one therefore occurs after n+2 clock cycles and all proceeding serial data bits are also logic high. The point of transition of the D-latch output state enables the phase offset period t_d to be deduced within the region $2\Delta t \leq t_d < 3\Delta t$. The phase measurement scheme can also be carried out for the case where $f_{ref\_clk} > f_{clk\_in}$ as shown in figure 4.5. The D-latch input trigger edge clk_in must however lag ref_clk by one period for each measurement since detection D0 will be zero always unless $t_d = 0$. This is achieved simply by ensuring that ref_clk is always triggered ahead of clk_in, i.e. by triggering ref_clk on the $(n+1)^{th}$ clock cycle. In addition, the output serial data bits must be reversed in order that the position of the rising clock edge corresponds to its actual position in time.

To conclude the phase measurement technique, the key points are summarized below to define parameters and the constraints that must be followed in order for the phase measurement scheme to function correctly. The structure presented in figure 4.3 is both simple with respect to its hardware requirements and also enables the phase measurement resolution (Δt) to be dependent on the frequency difference between ref_clk and clk_in. The proceding section develops this scheme to make it feasible for a TOA range measurement system that meets the control, timing and synchronization constraints introduced by WSNs.

1. Ref_clk must always trigger following the trigger edge of clk_in to ensure correct operation of the technique (serial output states will remain unchanged otherwise).

2. If $f_{clk\_in} > f_{ref\_clk}$ then serial output data bits are read from left to right and the D-latch output starts from the n^{th} rising clock edge.

3. If $f_{ref\_clk} < f_{clk\_in}$ then serial output data bits are read from right to left and the D-latch output starts from the $(n+1)^{th}$ rising clock edge.

4. Phase measurement resolution $\Delta t = |t_A - t_B|$, where the resolution of the phase measurement is dependent on the frequency difference between clk_in and ref_clk.

5. If $f_{clk\_in} = f_{ref\_clk}$ or $f_{clk\_in} = 2nf_{ref\_clk}$, where n is any positive integer value, phase measurement cannot be obtained.

6. One and only one logical output may be obtained per synchronization period to avoid aliasing.

7. The length of the synchronization period is dependent on the phase measurement resolution Δt, where increased resolution leads to an increased synchronization period and phase estimation period.

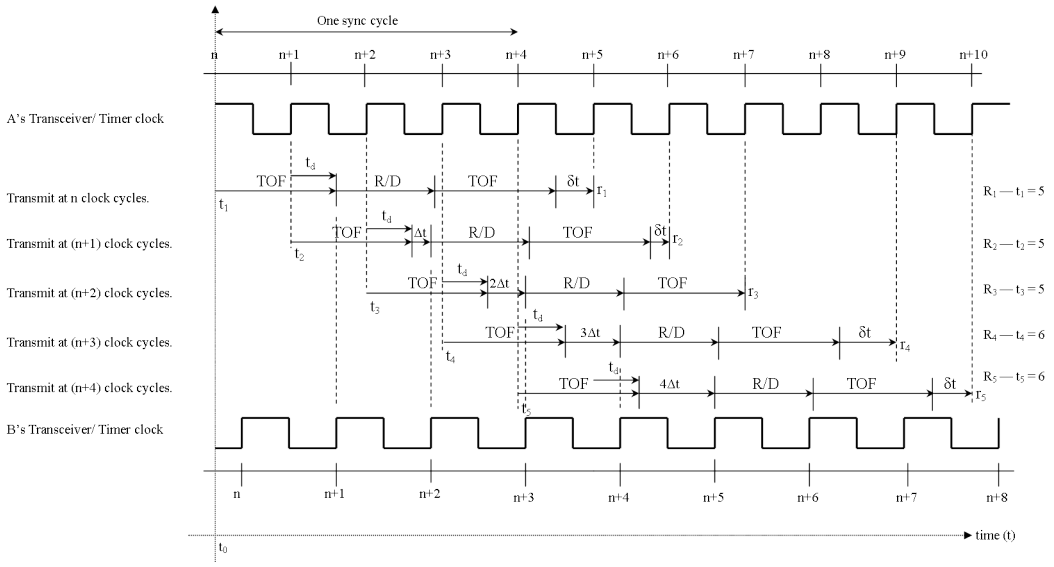


FIGURE 4.6: Timing diagram of two-way time-of-flight ranging with sub-clock phase offset measurement.

The constraints involved with TOF ranging, the time dependent VDL and WSNs must be combined in order to produce a high resolution ranging technique for point-to-point distance estimation. It has been shown that in order to perform TOF ranging measurement, the transmitter and receiver must be precisely synchronized in time. Furthermore, the resolution of TOF range estimates is constrained by the time quantization introduced by the round-trip timer clock. The use of the VDL principle enables this limitation to be removed, thus TOF ranging can be achieved within the constraints of sensor nodes including low frequency system crystal oscillators, hardware limitations and power consumption.

Time of Flight Ranging Technique

To satisfy the synchronization requirements between two devices involved with TOF ranging, two-way ranging transaction is used to perform unsynchronized TOF measurements as illustrated from a time perspective in figure 4.6. Devices A and B operate from clocks with known periods t_1, t_2 where Δt is the difference in period. The synchronization period is defined as the number of cycles of clock A for which A and B are out of phase as shown in figure 3.1. Two-way ranging transactions are exchanged between the devices for each incremented period of clock A to obtain sub-clock period phase measurements over the synchronization period. The scheme operates by devices A and B first committing to perform TOF ranging and agreeing a common RF channel by the exchange of initialization packets. Following this stage, two-way ranging transactions are made between A and B. Device A transmits a ranging message to device B. During transmission, A reads and stores the value of a free-running timer. After a TOF propagation period corresponding to the distance AB, the message arrives at B, which receives this message on its next clock edge after $n\Delta t$, where n is the phase measurement number. After a fixed period response delay (R/D), B transmits a ranging transaction

back to A. Following the return TOF period, A receives the ranging message after a period δt and again stores the value of the free-running timer. The two-way period is determined by subtracting the final stored value from the initial stored value. This process is repeated with each two-way measurement shifted in time by one clock period over the synchronization cycle to obtain the round-trip estimates including a phase offset term. The period δt does not affect phase measurements since its period is always less than one cycle of A's clock. Phase measurement resolution Δt is decided by the frequency difference between A and B where Δt is incremented for each measurement by transmitting on the next successive clock edge. Phase offset can also be determined more efficiently by either using multiple one-way transactions followed by one return transaction or by two-way measurements timed at both A and B. The TOF period with phase offset measurement t_d is then computed by finding the arithmetic mean described by equation 3.4 for n measurements over the synchronization period. This estimate is then converted to a distance estimate by executing three steps: (1) obtaining the calibrated round-trip period by subtracting the minimum round-trip period (when the distance A-B is zero) from the mean estimate round-trip period; (2) obtaining a single TOF period by dividing the calibrated estimate round-trip period by 2; (3) using the relationship $\Delta s = v\Delta t$ to convert from time to distance. The resolution and constraints of this ranging method are summarized by the following key points:

1. TOA ranging resolution can be measured to as low as the time period of As transceiver/ timer clock if both A and B are the same frequency.

2. If $f_A = f_B$ or $f_A = 2nf_B$, where n is any integer value, phase offset measurement cannot be obtained.

3. Phase measurement resolution is determined from $\Delta t = |t_1 - t_2|$, where the resolution of the measurement is dependent on the frequency difference between devices A and B involved with the TOA ranging.

4. The frequency of device A (f_A) and frequency of device B (f_B) should be continuous over all two-way measurements.

5. Successive measurements must be offset in time by one clock period for each measurement over the synchronization period in order to measure phase offset.

6. Only a single round-trip period may be obtained per synchronization period to avoid aliasing.

7. Finding the mean round-trip estimate removes any uncertainty caused by $f_A > f_B$ or $f_A < f_B$.

4.2 System Implementation

4.2.1 Prototyping platform

A Texas Instruments (TI) CC2430 development kit [33] consisting of two SmartRF04EB boards was selected to prototype the two-way TOF ranging system. The TI CC2430 is a fully integrated 2.4 GHz RF transceiver and Intel 8051 Microcontroller unit (MDU) particularly suited for WPAN applications compliant with Zigbee and IEEE 802.15.4 communications protocol. The RF radio module operates with Direct Sequence Spread Spectrum (DSSS) modulation and a 2 Mb/s chip-rate to produce a 250 kb/s data rate in the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band [29]. To extract round-trip timing for TOF measurements, the TI CC2430s high-frequency 32 MHz crystal oscillator and MAC capture timer are used. The ranging algorithm is fully software based and the TI CC2430 development kit is unmodified with no additional hardware overheads. Figure 4.7 shows the high level block diagram of the TI CC2430 RF transceiver. Data is transmitted by the CC2430 direct conversion modulator by first buffering up to 128 bytes in to a first-in-first-out (FIFO) data buffer. The IEEE 802.15.4 compliant preamble and start-of-frame-delimiter for packet identification and synchronization are generated in hardware and added to the start of the data packet. Each set of 4 bits (defined as a symbol) of the packet are then mapped according to the corresponding IEEE 802.15.4 32-chip pseudo-random spreading sequence [29] and output to the digital-to-analogue-converters (DACs). Sub-symbols are called chips to differentiate them from bits (information) and symbols (collections of bits) [63]. This digital process implements a DSSS scheme with a chip rate of 2 M Chips/ sec. The transmit signal is generated using single step I/Q-up-conversion where the modulated and spread I/Q baseband signals are low-pass filtered and up-converted directly to RF by a single-band modulator. The RF signal is finally amplified to a programmable level by the power amplifier (PA) and fed to the external antenna.

On reception of data, it is first passed through a low noise amplifier (LNA) and down-converted in quadrature (I and Q) to a 2 MHz intermediate frequency. The separate I and Q signals are then band pass filtered and amplified before being digitalised by the analogue-to-digital-converters (ADCs) and passed to the digital demodulator. Here, a final digital process is used to perform final channel filtering and recover the signals data by despreading, symbol correlation and byte synchronization [55]. Switching between transmit and receive modes of operation is handled internally on the TI CC2430 via software. The TI CC2430 modulation format is compliant with IEEE 802.15.4 and is described fully in [29]. The process of modulation and spreading binary data is illustrated at block level in figure 4.8(a). Each data byte to be transmitted is divided into two 4-bit symbols. The four least significant bits (LSBs) of each byte are mapped to one symbol and the 4 most significant bits (MSBs) are mapped to the following symbol. Each symbol, in order is then mapped to (or used to select) one of 16 orthogonal pseudo-

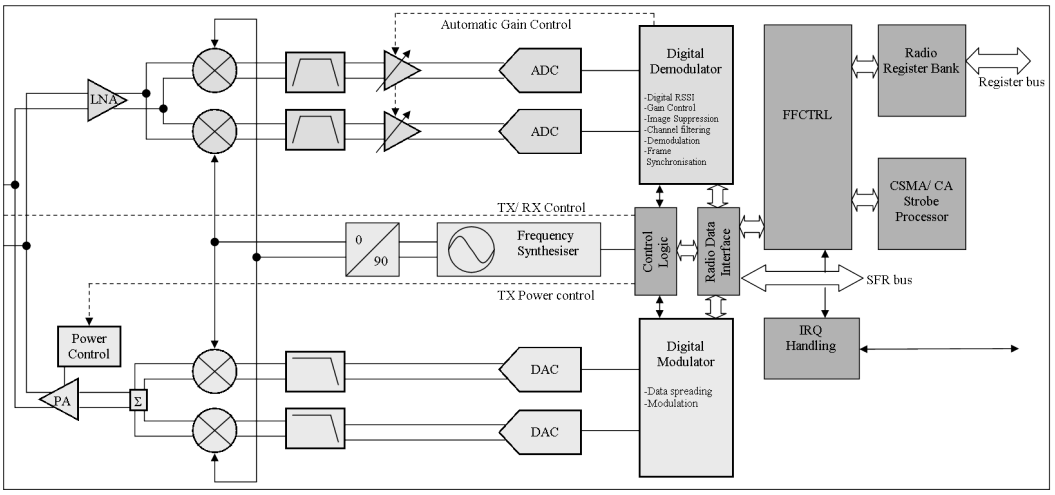
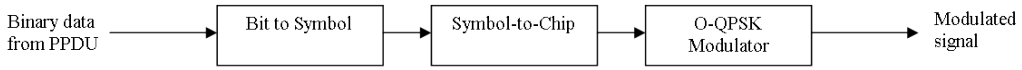


FIGURE 4.7: High level block diagram of TI CC2430 radio module (reproduced from [55]).

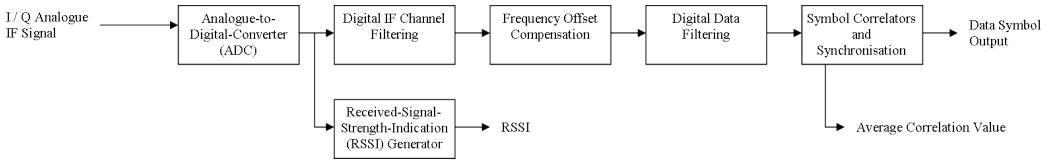
random spreading functions, 32-chips each. Those functions can be found in [29]. The chip sequences are then transmitted using O-QPSK modulation at 2 MChips/ second, with the least significant chip being transmitted first for each symbol. A schematic example of transmitting a zero symbol sequence is illustrated in [55]. Even indexed chips are modulated onto the in-phase (I) carrier and odd-indexed chips are modulated onto the quadrature-phase (Q) carrier with half-sine shaping. To form the offset between the I and Q-phase chip modulation, the Q-phase is delayed by T_c with respect to the I-phase chips, where T_c is the inverse of the chip rate [55]. The TI CC2430 signal demodulator is shown in figure 4.8(b). Channel filtering and frequency offset compensation are performed digitally. Digital data filtering is performed at chip level with the demodulator making a decision for each received symbol using over-sampling symbol correlators to despread the 32-chip pseudo random functions. A continuous start-of-frame-delimiter (SFD) search is used to achieve symbol synchronization, where, on detection proceeding data bytes are written to a FIFO receive buffer. This data may then be read out by the MCU at a lower bit rate than the 250 kbps generated by the receiver [55]. Symbol re-synchronization is also performed to adjust for the error in the incoming symbol rate in order to reduce performance degradation of the demodulator. RSSI and symbol average correlation value outputs are also generated to provide estimates of the signal level in the channel and LQI [55]. The TI CC2430 transceiver is half-duplex, it can only be in either transmit or receive mode of operation at one time, however, this does not interfere with the process of two-way TOF ranging.

4.2.2 Frame format and timing extraction

The TI CC2430 supports the IEEE 802.15.4 frame format described fully in [29] consisting of a synchronization header (SHR), PHY header AND PHY service data unit (PSDU). Its compliant adaption for TOF ranging is shown in figure 4.10 as transmitted



(a) TI CC2430 modulation and spreading functions block diagram (reproduced from [55]).



(b) TI CC2430 demodulator block diagram (reproduced from [55]).

FIGURE 4.8: TI CC2430 Modulator and Demodulator block diagrams.

by the PHY layer from left to right. The synchronization header consists of a preamble sequence for 4 bytes followed by a a single byte start-of-frame-delimiter (SFD). The length of the preamble can be configured for systems non-compliant with IEEE 802.15.4 communications protocol [55]. During receive mode, the synchronization header is used by the transceiver signal demodulator to identify and synchronize to the incoming data frame. On reception, the transceiver frequency adjusts and synchronizes to the received preamble sequence. Compliant packets are identified by a continuous search and correlating the received preamble sequence with a local copy. The frame length field is implemented to make data frames compliant with IEEE 802.15.4 but is not essential for TOF ranging packets. To make the IEEE 802.15.4 frame efficient and suitable for TOF ranging measurements, only the synchronization header, PHY header and a PSDU consisting of an identifier, address information and check sequence are used. This corresponds to ranging packet which are 11 bytes in length. The IEEE 802.15.4 acknowledgement frame can be used optionally to verify the successful reception and validation of a data or MAC command frame. If the receiving device is unable to handle the received data frame for any reason, the message is not acknowledged [29]. It is expected that this ranging frame format and the IEEE 802.15.4 acknowledgement frame format could be combined in order that two-way ranging is integral with the 'acknowledgement' process used in IEEE 802.15.4, thus adding no increased data transmission overhead and providing the synchronization overhead of this TOF ranging algorithm.

In chapter 3 the limitation of ranging performance were detailed, those include SNR, signal bandwidth and code duration. The important point here is that only the preamble sequence length in an IEEE 802.15.4 packet is significant for TOF ranging. Each symbol, half a byte in length has a 32 us duration. The length of the preamble sequence can be configured over a range of 1-16 leading zero symbols through the TI CC2430s MDMCTRLLOL.PREAMBLE_LENGTH register [55]. For compliance with IEEE 802.15.4, a preamble sequence of 8-symbols of zeros is used for this ranging system. By the derivation in chapter 3, this corresponds to a ranging accuracy of 7.46 m for a single two-way ranging estimate. Table 4.2 summarizes the expected lower bound range accuracies for a single two-way transaction assuming an average SNR of -20 dB and using different configured preamble sequence lengths. Note that the improvement to ranging performance

TABLE 4.2: Expected lower bound variance for a single range estimates using IEEE 802.15.4 with different preamble sequence duration.

Preamble length (bytes/symbols)	Duration [us]	$t_s \cdot B \cdot SNR$	σ_{TOF} [m] (two-way)
4/8	256	5.12	7.46
6/12	384	7.68	6.09
8/16	512	10.24	5.28

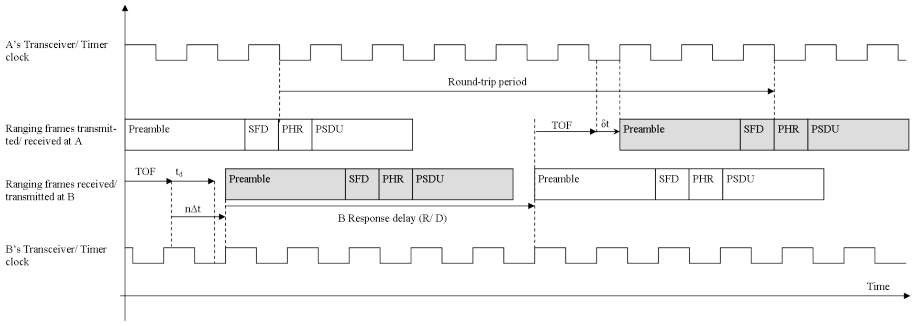


FIGURE 4.9: IEEE 802.15.4 frame perspective time diagram for two-way TOF ranging. System elapse periods described from the perspective of frame transmit and receive. Transmitted ranging frames denoted by white, received ranging frames denoted by grey, where t_d denotes the phase offset between A and B.

is non-linear as with averaging more samples and in essence, code duration is effectively averaging.

Timing extraction for TOF estimation is provided through the SFD byte. On reception and synchronization of compliant packets, the SFD byte triggers timing extraction via a free-running timer. The TI CC2430 incorporates a 16-bit MAC timer which is configurable to capture the rising edge of the SFD on transmission and reception of ranging frames. This is configured to free-run and the round-trip period is extracted by subtracting the final timer value from the initial timer value. Switching between transmit and receive mode of the transceiver is performed through software for each two-way measurement. The two-way packet transfer process is illustrated from the time perspective in figure 4.9 for the transmission and reception of IEEE 802.15.4 adapted ranging packets.

4.2.3 Software algorithms

Software algorithms are fully developed in C using the IAR compiler [77] and flash programmed on to the TI CC2430 via the development board using the Chipcon flash programmer. There are no implemented network layers because the focus of this research is primarily on ranging which is simple and does not require complex networking structure for its development and operation. Ranging is performed between two TI CC2430

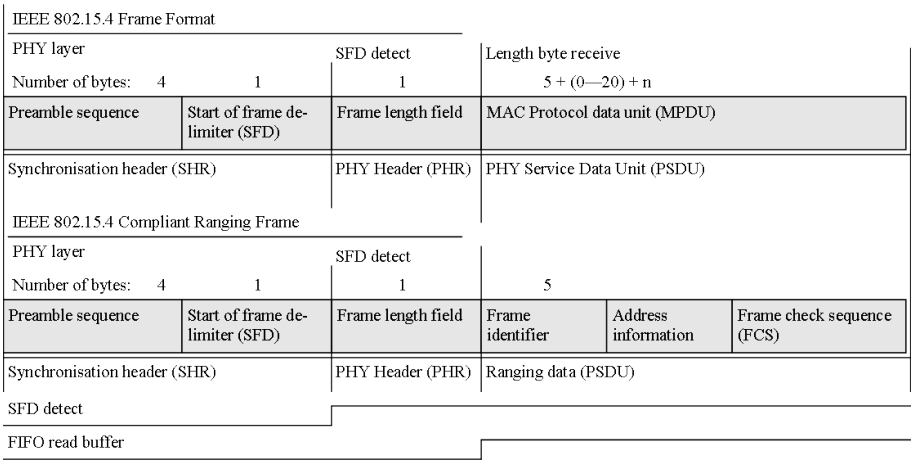
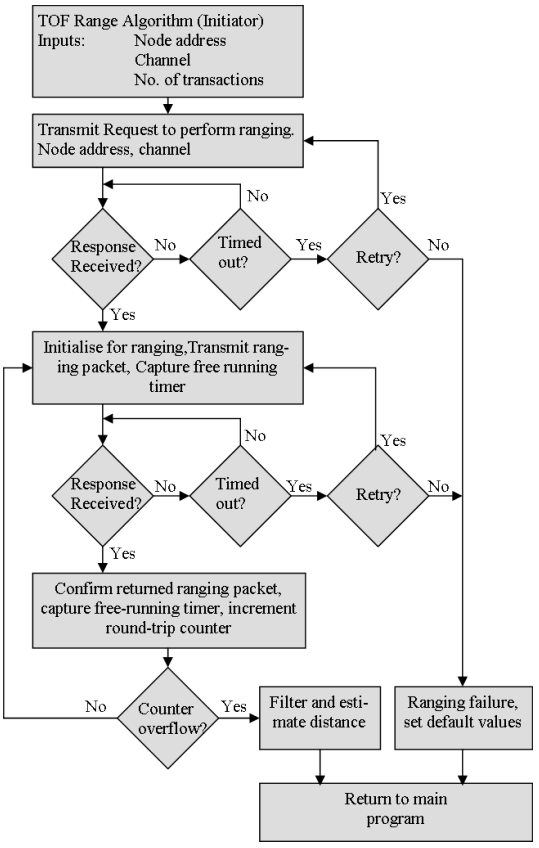


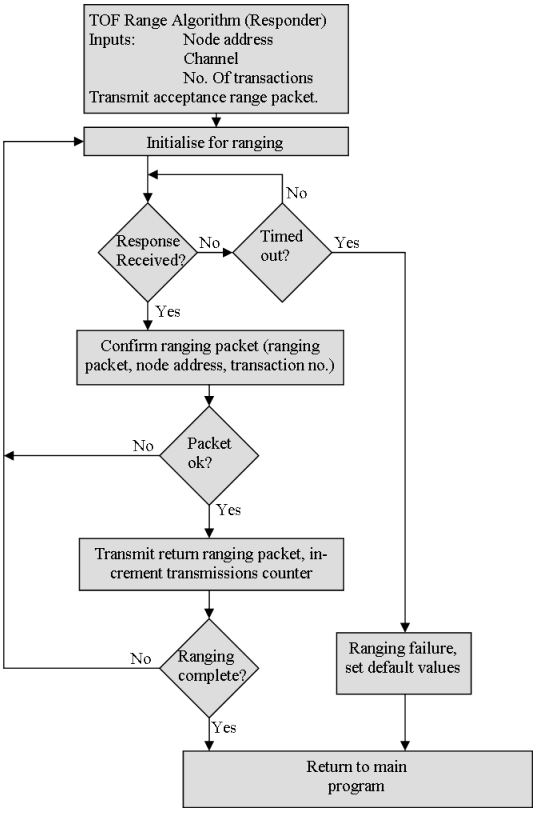
FIGURE 4.10: Schematic illustration of IEEE 802.15.4 Compliant Ranging Frame.

development platforms which are flash programmed independently as an 'initiator' and 'responder'. For the purpose of testing, the address of the responder and the number of ranging transactions to be executed are pre-programmed on to the initiator prior to the ranging process. A ranging packet identifier is also predefined as a single byte. High level software flow diagrams for the initiator and responder are shown in figures 4.11(a) and 4.11(b). Both the initiator and responder are identical in terms of hardware and only the software algorithms for the ranging process are different. Therefore, either of the TI CC2430 development platforms can be used as the initiator and responder. To initiate the ranging process, the initiator device A requests to perform ranging with the responder device B by transmitting a 'request to range' (RTR) packet. Assuming that device B is within radio range of A and the packet is not lost, B receives and acknowledges the 'request to range' message by transmitting an 'acceptance to range' (ATR) packet back to A. Assuming arrival of the ATR packet at A within an appropriate time period, A and B both initialize to perform ranging. The RF radio is configured and the agreed channel for ranging is selected. The round-trip timer is configured to operate as a free-running capture timer with capture activated by the rising edge of the SFD detect. A ranging packet is then transmitted to B with the value of the free running timer captured on transmission. Device A switches to receive mode and waits for a return ranging packet from B. If the return ranging packet is not received within a time-out period, the ranging transaction is presumed 'lost' and the ranging packet is re-transmitted. Three re-transmission attempts are made before the ranging process is regarded as a 'failure'.

On reception of a packet at device A following previous transmission of a ranging packet, the packet preamble sequence and SFD trigger the capture of the free-running capture timer. Device A checks the identity of the packet and if as expected (i.e. a ranging packet), the round-trip measurement is calculated by subtracting the transmit time from the receive time. This value is stored and the ranging transaction counter is incremented to indicate the number of successfully completed ranging transactions. If a corrupt or incorrect packet is received, the round-trip measurement is disregarded.



(a) Flow diagram for 'initiator' device.



(b) Flow diagram for 'responder' device.

FIGURE 4.11: Software flow diagrams for 'initiator' and 'responder' devices involved with two-way ranging.

The process is repeated until the required number of ranging transactions have been achieved. The distance estimate with phase offset measurement is then computed and filtered as required. Ranging is complete and the estimated distance is returned to the main program.

From the perspective of the responder B. A 'request to range' (RTR) packet is received from device A. This packet contains the address of the device A which is requesting to range with B, the channel on which ranging should be executed and the number of ranging transactions to be performed. Assuming device B has the corresponding packet address, the ranging process can be executed. B acknowledges the RTR by transmitting an 'acceptance to range' (ATR) packet back to A and then enters a waiting loop ready for a ranging packet to be received from device A. If no ranging messages are received within the waiting loop, i.e. the ranging packet is lost, the loop times-out and the ranging process is regarded as a failure. The radio module and round-trip timer are returned to their default values before the ranging algorithm is exited. The main program receives a set of standard values in the case of a ranging failure, i.e. pre-defined values which represent a ranging failure. Alternately, when a packet is received, B confirms the packet type, checks its validity and stored the transaction number. If the parameters are as expected, B transmits a return ranging packet back to A. This process is always executed over the same number of system clock cycles in order that the phase offset can be obtained. Alternately, if the received packet is corrupt or of an incorrect type or format, B returns to its waiting loop ready to receive the next ranging packet. Following completion of all ranging transactions, B returns all hardware device values to their defaults and jumps back to the main program.

4.2.4 Interference issues

The two-way TOF ranging system is prototyped using the TI CC2430 which uses an IEEE 802.15.4 compliant communications protocol and operates in the 2.4 GHz ISM band. It is expected that other wireless systems will interfere in this band including 802.11b/g WLAN. To avoid interference, a clear-to-send channel check is made before transmission of ranging packets. If a ranging packet becomes corrupt or is lost, the two-way transaction is disregarded and an additional transaction is made to complete the data set. To further avoid interference issues with the prototype system, i.e. because interference mitigation techniques have not been implemented, testing is carried out in remote locations where interference sources are minimal during testing the prototype system. During the process of ranging in a network of an arbitrary number of nodes, the collision of ranging and data packets may be avoided by either performing ranging on a different RF channel to that of the data transfer, using allocated time slots or by random delay between transmission of packets.

4.2.5 Error margin

MacCrady et al [74] define the error margin as the sum of all the variances of each time delay period of the transceiver components as a TOF ranging signal passes through them. The total time delay (T_{delay}) is a Gaussian random variable formed by summing each of the independent components and is defined by equation 4.1 were its variance is reduced by N two-way transactions (i.e. $\sigma_T^2 = \sigma_{t_i}^2/N$).

$$T_{delay} = \frac{1}{N}\sum_{i=1}^{N}(t_i),\ where\ i = 1, 2, ..., N \tag{4.1}$$

For a single two-way ranging transaction, the total time delay consists of both a transmission and reception at the initiator and responder (with antenna delays), a relative phase offset term between device clocks and a response delay period. This is defined by equation 4.2, where t_{1T}, t_{2T}, t_{1R}, t_{2R} are the transmission and reception times at the initiator and responder, Δt_2 is the relative phase offset and t_{2RES} is the response period.

$$T_{delay} = t_{1T} + t_{2R} + \Delta t_2 + t_{2RES} + t_{2T} + t_{1R} \tag{4.2}$$

If multiple two-way transactions are performed, then the variance in TOF estimates is expected to reduce by a root function of the number of transactions. The corresponding error margin of equation 4.2 is expressed by equation 4.3. It is clear from 4.3 that error in TOF estimates can be reduced either by multiple two-way transactions or by reducing the variance in individual time components. Considering that the TI CC2430 components cannot be independently accessed to measure individual time delays, several assumption can be drawn based on equation 4.3 before proceeding: (1) the time variance from the transceiver's analogue front end for both the receiver and transmitter including antenna delays is expected to be less than one nano-second, as reported in [74]; (2) the relative phase offset between the initiator and responder will contribute the greatest error; (3) the error contribution from the response delay will also be less than 1 ns given that the crystal oscillator accuracy is typically 40 ppm of the crystal frequency for the TI CC2430.

$$\sigma_{TOA} = \frac{1}{\sqrt{N}}[\sigma_T + \sigma_{R2} + \sigma_{\Delta t2} + \sigma_{t2RES} + \sigma_{T2} + \sigma_{1R}] \tag{4.3}$$

To verify those assumptions, figure 4.12 shows the capture of the SFD over successive receptions of data packets using the TI CC2420 in place of the TI CC2430 because of the readily available hardware and direct access to the SFD through hardware. The transmitting TI CC2420 is used as a trigger for the digital storage oscilloscope (DSO) , and the SFD rising edge of the receiving TI CC2420 is captured by the DSO on reception

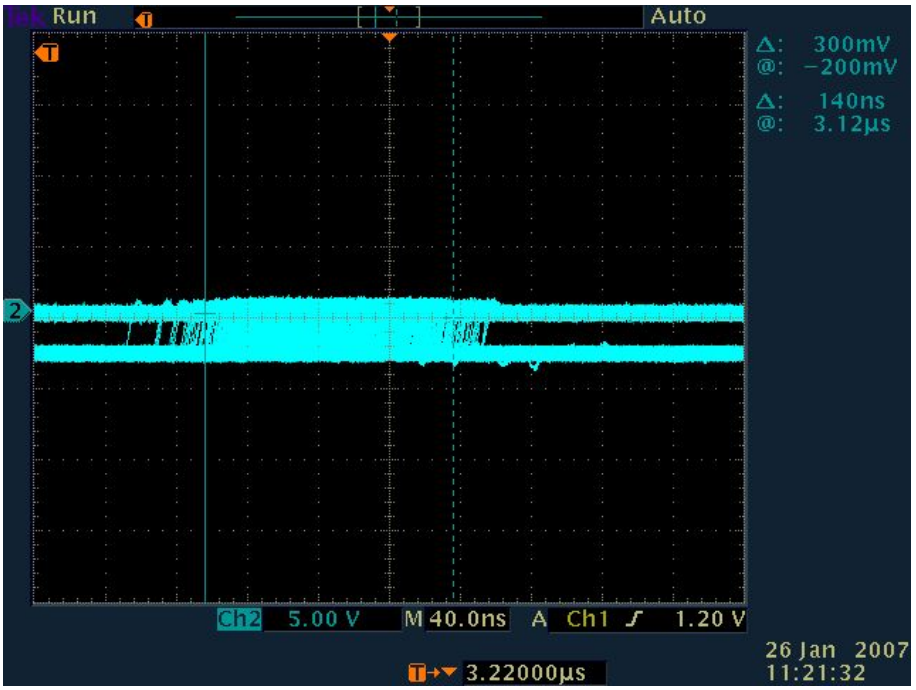


FIGURE 4.12: Signal correlator drift capture over 125 ns period for TI CC2420. Continuous transmission and reception of packets. Drift captured by capturing rising edge of start-of-frame-delimiter pin using digital storage oscilloscope and transmitting device as a trigger.

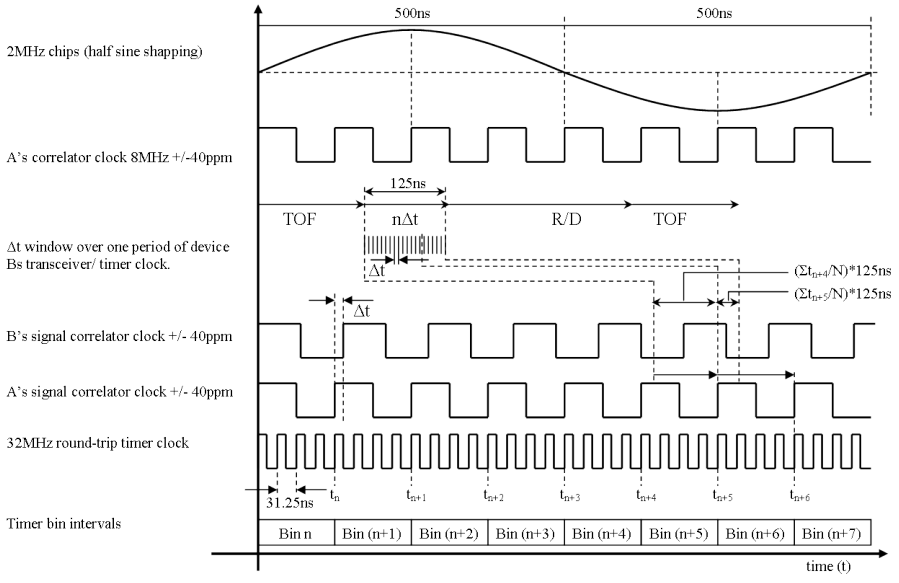


FIGURE 4.13: Two-way ranging with sub-clock phase offset measurement using the TI CC2430.

of data packets; hence, figure 4.12 shows the variance contribution of $t_{1T} + t_{1R} + \Delta t_2$. Since t_{1T} and t_{1R} are expected to be small (i.e. $<$ 2-3 ns), figure 4.12 confirms that the TI CC2420 correlates incoming chip sequences at 8 MHz (1/125 ns) given the approximate 125 ns drift period. The 140 ns period of drift is expected from t_{1T}, t_{1R} and early and late arrivals through multipath propagation during laboratory testing. Figure 4.13 illustrates

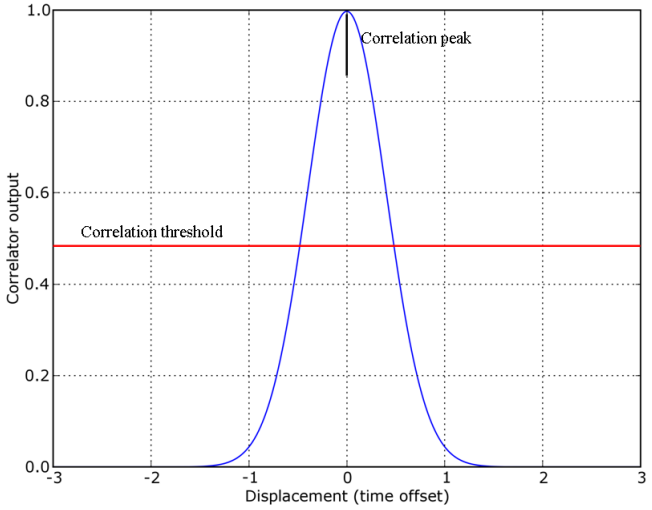


FIGURE 4.14: Output function of auto-correlation of two similar signals.

a simplified timing diagram for the two-way ranging scheme using the TI CC2430. TOF ranging packets are transmitted using half-sine shaped chips with frequency 2 Mchips s^{-1}. The drift period measured in figure 4.12 confirms the receiver's signal correlation period as 125 ns (8 MHz) in order to detect the half-sine shaped chip sequences. To carry out round-trip timing using the TI CC2430, a MAC capture timer is used which has a frequency of 32 MHz. This is a factor of four times the correlation frequency and hence it is expected that the histogram bars will be separated by four clock periods for each round-trip time measurement. Although this does not affect the performance of the two-way ranging system, the quantization error will increase the number of transactions necessary to obtain a specified ranging accuracy. Based on the result from figure 4.12 and the relative frequency difference between two TI CC2430 development boards, Δt is too small to measure using an oscilloscope and would require the use of a frequency counter for its measurement. Therefore the assumption is made that relative phase offset between the initiator and responder is sufficiently random in order that the drift distribution can be considered normal. This corresponds to the initiator and responder having a random offset phase difference Δt. Under this assumption, ranging accuracy, in the absence of noise, is expected to be $\sigma_x^2 = 18.75/\sqrt{N}$, where N is the number of transactions (i.e. d=vt $\rightarrow$ (3 x 10^8).(125 x 10^{-9}) = 37.5 m, two-way $\rightarrow$ 37.5/2 = 18.75 m/ clock period). Therefore, theoretically through the use of interpolation of round-trip range measurements, the resolution of the system can be improved up to the noise limit.

Signal Correlation

Ranging systems that utilise large spectral signal bandwidth (i.e. UWB) must precisely estimate the TOA of the ranging signals rising edge to meet the accuracy requirements of precise ranging. Therefore all the information on the TOA is within a very short time interval ($<$ 10 ns). In contrast, narrow-band ranging systems must extract the precise

TOA from a periodic pseudorandom waveform where the TOA is contained over the entire waveform. The phase difference between the receiving periodic ranging signal and a local copy of this periodic waveform at the receiving device must be precisely measured to improve range estimates. Therefore, multiple TOA estimates can be performed over the entire periodic waveform in order to improve the TOA estimate and enable precise timing of better than 3.3 ns required for a ranging system in WSN applications. The TI CC2430 receiver down converts received ranging signals from the 2.4 GHz RF carrier, base-band filters and amplifies the signal before quantizing its analogue value to its corresponding digital state. The quantized signal is digitally compared with the local copy by performing auto-correlation at symbol level over the first eight symbols of the received signal [55]. The correlation function is essentially a convolution function which operates by sliding a periodic local copy across the first eight symbol periods of the received signals and recording the sum of the product of the correlated symbol sequences at each offset [63]. The resultant correlation function is illustrated in Figure 4.14, where a maximum exists when the phase difference between the received signal and the local copy is minimum. The TI CC2430 incorporates a minimum and maximum threshold for the correlation process to reduce the detection of non-compliant and severely errored packets. A correlation value of 110 indicates a maximum quality correlation in contrast to a value of approximately 50 indicating a poor correlation and lowest quality of frame detectable using the TI CC2430 [55]. However, a high correlation threshold in the absence of noise can be used to limit the maximum phase offset of TOA ranging signals and it is expected that the quantized correlation threshold provided by the TI CC2430 can be used to improve TOA estimates. Determining the TOA time offset during auto-correlation is beneficial in reducing synchronization time error and obtaining more accurate sub-clock phase measurement. If the relative phase offset between the initiator and responder is considered to be uniformly random, the error induced through phase offset contributes only further noise and thus has no significant effect on ranging performance. However, uniformly random clock phase difference between the initiator and responder is challenging to achieve and thus it is more practical to consider the accurate generation of Δt. If Δt is precisely generated then the time offset between the TOA estimate and the true TOA must be more accurately estimated to improve the performance of the ranging system. To quantify this time offset error, the TI CC2430 correlates received 2 Mchip/sec at 8 MHz. The coherence time is thus 16 ns corresponding to a ranging error of 4.8 m. Figure 4.15 illustrates a technique to reduce the time error contribution between the quantized correlation peak and the true TOA time. The received waveform is measured at four discreet time intervals introduced by the receiver quantization process. A closer approximation of the true peak is estimated by obtaining the intersection of the two lines calculated from the quantized values as illustrated.

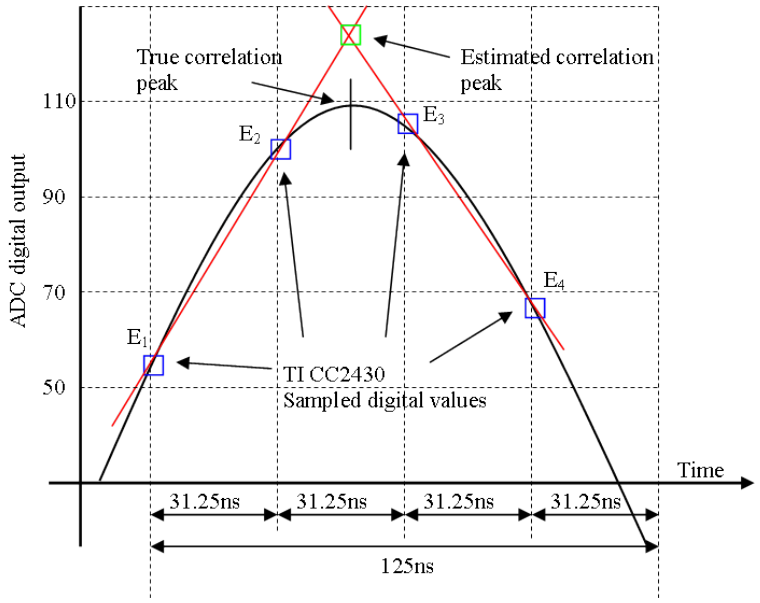


FIGURE 4.15: Diagram to illustrate correlation error and method to correct for this time offset.

4.3 Discussion and Summary

As discussed in chapter one, this ranging algorithm is intended for industrial, scientific and medical applications where the sensor nodes are of low cost, standard with respect to hardware architecture, processing abilities and communicate using low-power narrow-band radios such as those utilises for both IEEE 802.11 and IEEE 802.15.4. More specifically, the TOF ranging algorithm prototyped herein requires that the narrow-band radios use long duration, pseudorandom chip sequences for data transfer across the wireless channel which are auto-correlated with a local copy. They must also have both transmit and receive (transceiver) capabilities to enable TOF ranging with sub-clock phase measurement to be performed. The narrow-band radio modules in question must also utilise a start-of-frame delimiter (SFD) byte following the pseudorandom preamble chip sequence of a ranging packet for packet synchronization and timing capture. Thus, a suitable method to extract timing information must exist such as a capture timer (timer triggered on detect of SFD byte) with period of at least twice that of the signal correlator to enable sub-clock phase measurement. The hardware must also be able to switch between transmit and receive through software and in the required time periods to enable correct operation of the algorithm.

The following bullet points summarise the expected performance of the ranging algorithm herein based on the specific hardware used for the implementation of the prototype system:

- The TI CC2430 utilises a 250MB/sec data communications rate where chip sequences are correlated at 8MHz (four times the chip rate of 2Mb/sec). The 8MHz

signal correlator (correlating chips) limits the prototype system ranging resolution to 18.75 m (two-way ranging) when no algorithm is employed to mitigate this quantization.

- On the assumption that the relative clock phase offset between transceivers is normally distributed over multiple ranging transactions, ranging accuracy is improved by $\sigma_T^2 = \sigma_{t_i}^2/N$ for N ranging transactions. Therefore, if 100 two-way range estimates are performed and the mean is calculated, ranging accuracy is expected to be ± 1.88 m ($\sigma_{TOF} = 18.75$ m / $\sqrt{100}$) in the absence of noise and signal multipath.

- Ranging resolution is bound by Δt, where Δt is generated through the frequency difference between transceiver clocks involved with the TOF ranging process. In the current prototype system, Δt cannot be accurately controlled without further modification to the hardware. For this reason, the period Δt is assumed random and thus over multiple two-way ranging transactions, a normal distribution of range estimates is obtained. Based on this assumption, ranging resolution may be obtained up to the noise threshold of the system.

4.4 Results

Ranging results have been obtained for the LOS, NLOS and indoor environments using the standard TI CC2430 development kit operating on a single 2435 MHz channel and a transmission power of -1.5 dBm (700 uW). The LOS environment was a level grass field with no obstacles within 100.0 m of the test area. In contrast, the NLOS environment was on the University of Southampton Campus where buildings and foliage provided multipath, obstruction and signal blockage. Indoor testing was carried out in a residential flat constructed of brick work and stud-partition internal walls. Ranging was carried out over ranges of 250.0 m LOS, 120.0 m NLOS and 8.0 m indoors where the distances were restricted by boundaries of each test location. In order to extract a valid set of ranging data, a simple program was written in Python software to interface one of the TI CC2430 development boards to a laptop computer via its RS232 port and record the ranging data. To provide initiator-responder distance referencing for the LOS and NLOS tests, a XE1610-OEMPVT GPS receiver evaluation module was also interfaced to the laptop computer via one of the USB interfaces. The ranging measurement and GPS position estimates were then thread-read and recorded once per second each time a GPS position estimate became valid. Any corrupt samples (i.e. corrupt or lost ranging packets) were disregarded. The GPS receiver has an expected position accuracy of <5.0 m circular error probable (CEP) and resolution of 2.0 m by conversion of the latitude and longitude co-ordinates to metres. To confirm the conversion calculations, a measuring wheel was also used to measure the 250.0 m for the LOS condition. The accuracy of those techniques was considered satisfactory to reference the RF two-way

TOF ranging with the phase offset measurement algorithm. A 100 sample average was chosen arbitrarily per TOF measurement. This corresponds to an expected variance in ranging measurements of 1.9 m under ideal assumptions (i.e. random clock offset and in the absence of noise). Since GPS cannot obtain signal lock indoors, ranging estimates were measured in 1.0 m increments relative to a tape measure (maximum error less than 0.1 m). A high sample set of 1000 samples were used per measurement in order to achieve an expected variance in estimates of less than 0.6 m. To calibrate the ranging measurements, the minimum round-trip period was estimated over an average of 1000 ranging transactions when the transceivers were in close proximity (< 1.0 m). This average value was then subtracted from each ranging measurement before conversion to the distance estimates.

The TI CC2430 data sheet specifies frequency accuracy of ± 40 ppm for the 32 MHz crystal oscillator [55]. This frequency error is used to provide Δt between the initiator and responder for ranging experimentation. Further development of the prototype system (by modification to the hardware and clocks) would enable Δt to be more accurately generated. However, since the TI CC2430 development board operate using crystal oscillators with frequencies that drift in time, the relative drift between transceiver clock periods can be considered to be a random distribution. Thus, Δt is effectively a random time period due to drifting frequency in the crystal oscillators and noise factors. Given this assumption, and given that up to a ± 40 ppm frequency deviation can exist between the initiator and responder, a 1.25 ps time offset (40ppm) is a reasonable assumption for the frequency drift between each system clock cycle (31.25 ns $\cdot$ 40 ppm / 1000,000). Therefore in one second, the TI CC2430 initiator and responder system clocks will drift by 40 us (1.25 ps $\cdot$ 32 MHz) per second when frequency offset correction is not employed (in the case of TOF ranging). The drift offset period has boundaries 0 - 125 ns (one clock cycle of the signal correlator clock period) and assuming the aforementioned frequency difference Δt between the initiator and responder, ranging resolution is below 3.13 ns (125 ns / 40) time quantization when 40 ranging transactions are made once per second. This corresponds to ranging resolution better than one metre and the accuracy may be improved by averaging over greater numbers of sample sets. Thus, this derivation indicates that the accurate generation and calculation of transmission times limit the performance of this ranging system.

Figures 4.16 and 4.17 illustrate the linear ranging performance of the prototyped algorithm for the LOS condition over 250.0 m. The results confirm a typical improvement in ranging performance through averaging with an RMS error of 6.7 m. Resolution is typically 4.6 m because of the quantization introduced by averaging samples on the TI CC2430. Performance was consistent over the 250.0 m distance and performance only significantly degrading on reaching the limit of the TI CC2430 radio range which is as expected. The step-response of the GPS referencing in figure 4.17 typically shows that the distance referencing (GPS receiver) lost signal lock during test which introduces a

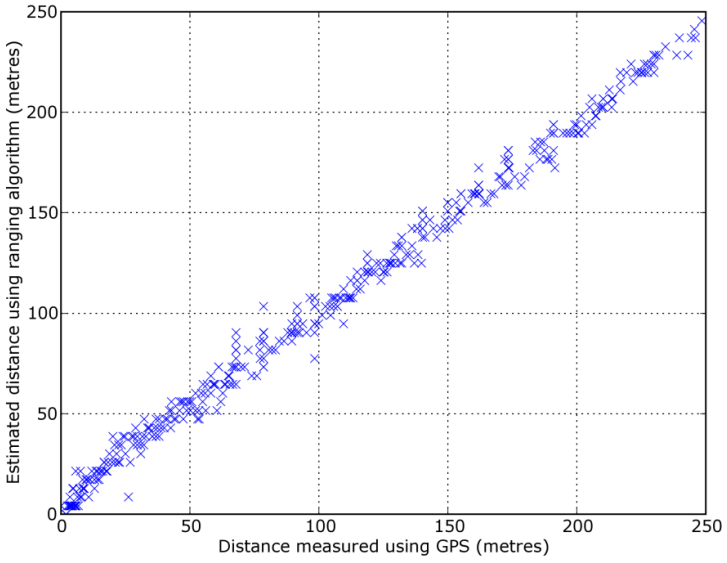


FIGURE 4.16: Performance of ranging algorithm for the LOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 7.0 m, max error = 24.9 m, min error = 0.0 m.

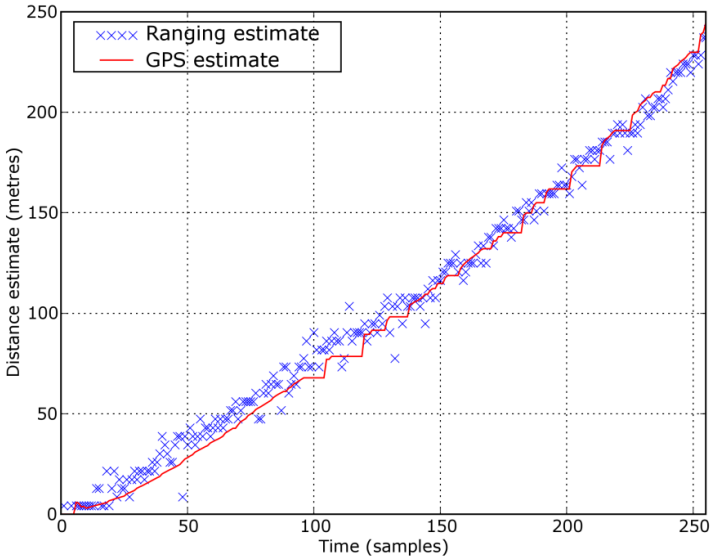


FIGURE 4.17: Performance of the ranging algorithm for the LOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

small error in the measured performance. One alternative frequency-dependent RF TOF ranging method [26] reports TOF ranging estimates with the RMS error of 0.9 m_{rms} and the peak error of 2.5 m for the LOS condition using a field programmable gate array (FPGA) and similar 2.4 GHz RF radio module. In comparison, this time dependent TOF ranging results inherit greater RMS error which is expected due to both the low averaged sample number and the inaccurately generated period Δt and unknown syn-

FIGURE 4.18: Photo showing LOS testing location 0.0 m - 250.0 m. Initiator node placed on tripod stand and interfaced to laptop computer for data extraction and logging. Responder moved across field with unobstructed signal path. March 2007.

FIGURE 4.19: Photo showing NLOS test location on University of Southampton campus. Initiator placed on tripod stand and interfaced to laptop computer for data extraction and logging. Responder moved around park area with obstructed and unobstructed signal path. March 2007.

chronization period using the prototype system implemented on off-the-shelf hardware.

Performance for the NLOS condition over 120.0 m is shown in 4.20 and 4.21 by moving the responder through different LOS, NLOS and complete signal blocked positions. The increased spread in ranging estimates illustrated in figure 4.20 confirms that the ranging system suffers more significantly in those conditions as expected. The RMS error is 15.8

m which is over twice the error reported for the LOS condition. This is expected not only for the aforementioned reason, but also due to the lost of GPS signal lock and the contoured landscape which was not accounted for with reference to GPS. NLOS ranging in [26] reports ranging results through a wall for fixed distance up to 10.0 m. The ranging error is 1.8 m_{rms} with a peak error of 3.4 m. It is expected that the significantly larger range error in this result is due to the larger transceiver-transceiver separation distance and NLOS signal propagation over the NLOS test environment.

A scale drawing of the indoor test environment is illustrated in figure 4.23. The initiator-responder separation distance is increased in 1.0 m increments over a total distance of 8.0 m with each estimate being computed for 1000 averaged samples. The sample number is increased to reduce the variance in estimates due to the short testing distance. Internal doors where left open during test and testing was carried out for the LOS condition through three rooms including a living room, hall and bedroom with full furnishings including tables, bookshelves, chairs, glass units and many other surfaces which contribute to signal distortion and scattering. Figure 4.24 illustrates ranging performance for the condition where the responder is placed at each known distance between 0.0 and 8.0 m. The ranging RMS error was measured as 1.7 m with a maximum error of 3.2 m. This compares well to the indoor LOS results reported in [26] where the ranging error was measured as 2.6 m_{rms} with a peak error of 5.5 m over similar transceiver-transceiver test distances. The results confirm that averaging greater sample numbers reduces TOF range estimate error as expected. Figure 4.25 shows the performance of the algorithm for real-time motion when the responder is linearly moved over a initiator-responder distance of 8.0 m. The RMS error was measured as 3.2 m with a maximum error of 6.0 m. The larger error was expected under velocity because of the time-variant channel. This is because the larger sample set makes the system exceed the maximum coherence time.

The results are summarized in table 4.3. Ranging accuracy is constrained by noise, quantization in the round-trip timing measurements and averaged sample number. Assuming a normally distributed clock offset (figure 4.12), the expected accuracies in the absence of noise, transceiver analogue front end (AFE) and signal lock delays are 1.9 m for the LOS and NLOS conditions using a 100 sample average ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 100$). Under the same assumptions, indoor accuracy was expected within 0.6 m using 1000 averaged samples ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 1000$). The addition of noise, signal multipath, AFE and transceiver signal lock delays increased this variance for each condition. Figure 4.12 confirms a 140 ns relative drift period; hence, it is expected that the variance in time delay from all additional contributions to be in the region 0-15 ns (140 ns - 125 ns $\rightarrow$ 15 ns, minus multipath delay from test environment), hence limiting the performance of this ranging technique. We expect those time variance contributions to be reduced by increasing the number of two-way ranging transactions.

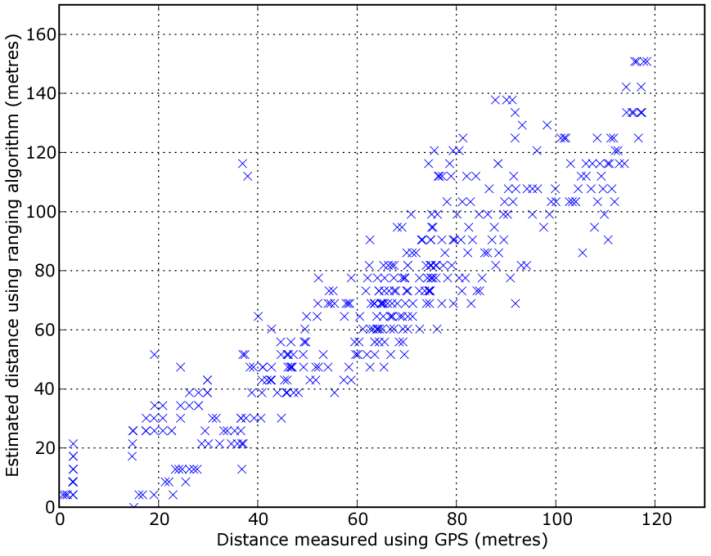


FIGURE 4.20: Performance of the ranging algorithm for NLOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 15.8 m, max error = 79.5 m, min error = 0.0 m.

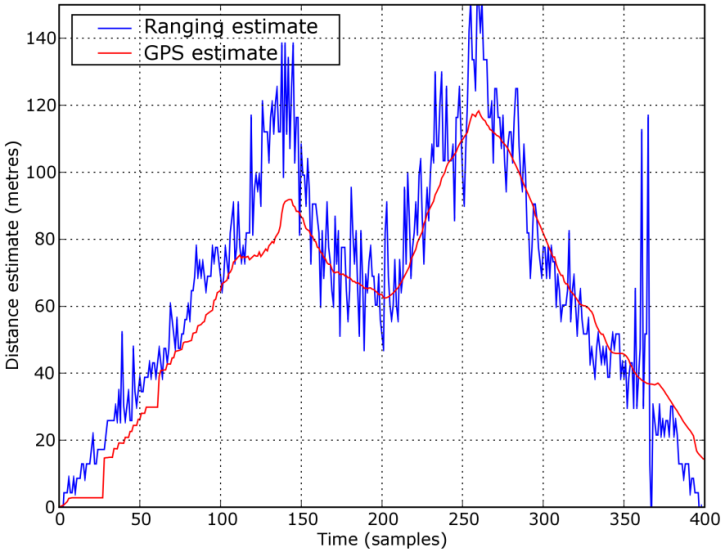
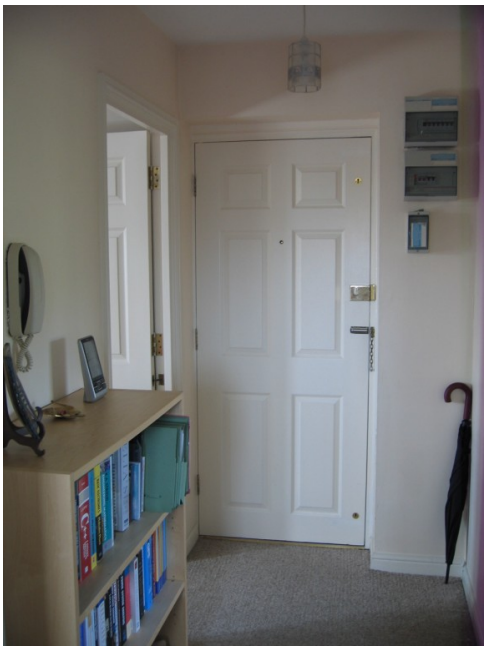


FIGURE 4.21: Performance of the ranging algorithm for the NLOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

For this technique to operate as expected, the assumption was made that the distribution of the relative clock offset between transceivers is normally distributed. Figure 4.26 illustrates the quantized distribution of the relative clock offset. This test was performed for 1000 round-trip TOA measurements where the initiator and responder were placed

(a) Photo of residential flat living room used to perform indoor ranging experiments. View from hallway towards living room window.



(b) Photo of residential flat hallway used to perform indoor ranging experiments. View from bathroom towards main entrance door.

FIGURE 4.22: Photographs of residential flat hallway and living room used for indoor ranging experiments. Rooms contain full furnishings. Walls constructed from stud-partition. Door made from solid wood.

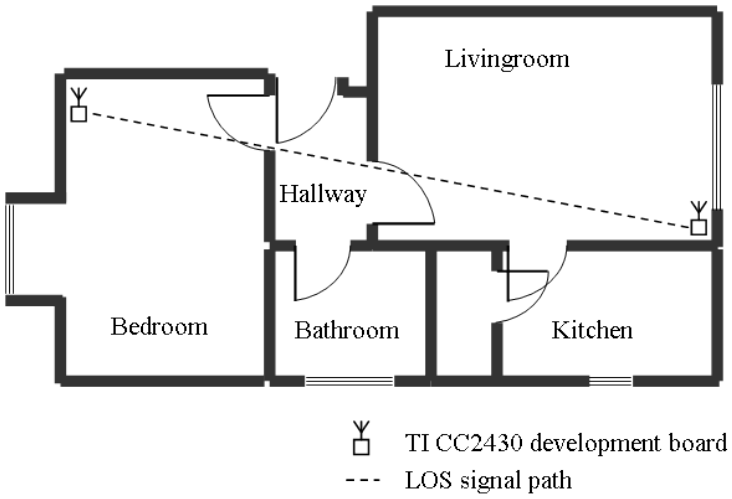


FIGURE 4.23: Scale diagram of the residential flat used for indoor testing of the two-way TOF ranging algorithm. External walls constructed using brick work; internal walls are stud-partition. Ranging experiments conducted for the LOS condition over 8.0 m with internal doors remaining open.

with antennas separated by 0.1 m. The signal correlator frequency was determined as 8 MHz, four times lower than the 32 MHz MAC timer used for round-trip timing, hence the histogram bars are expected to be spaced by four clock periods (i.e. at 22, 26, 30 and 34). The additional bars at 23, 27, 31 and 35 are expected to be caused by late triggering of the capture timer. In the ideal case (i.e. in the absence of noise and no

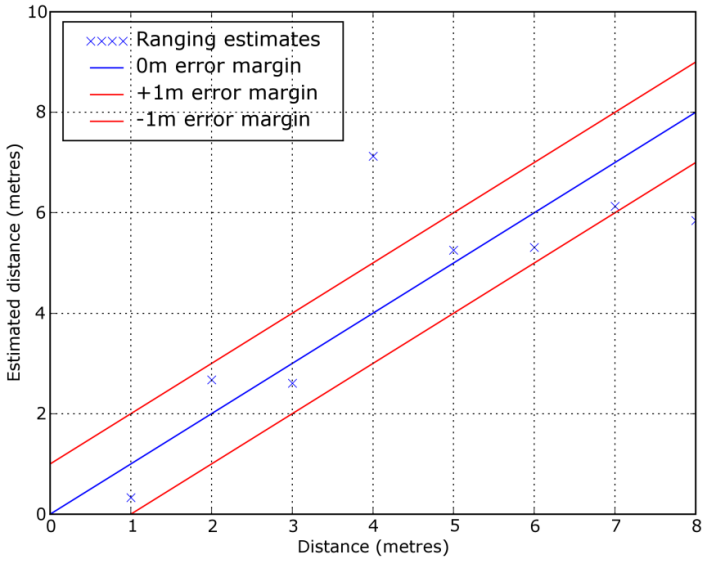


FIGURE 4.24: Performance of the ranging algorithm for the indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 1.7 m, max error = 3.2 m, min error = 0.3 m.

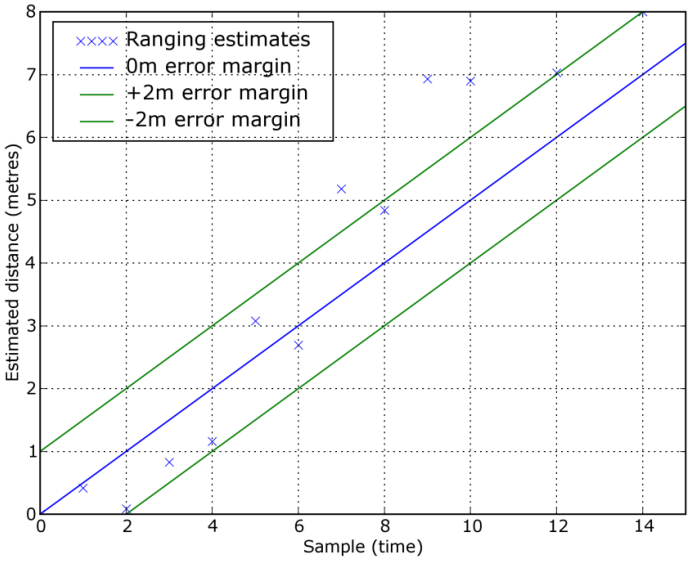


FIGURE 4.25: Real-time motion performance of the ranging algorithm for indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 3.2 m, max error = 6.0 m, min error = 0.0 m.

time delays in AFE) only two histogram bars would exist, however the additional bars are expected due to the 140 ns drift period shown in figure 4.12. It is expected that error is also caused by the non-ideal receiver lock on chip-sequences during reception as the receiver tries to synchronize to the packet preamble chip sequence. The results compare well with those expected based on system parameters detail in the summary. For a single range estimate, resolution is bound by the signal correlator period and therefore

TABLE 4.3: Prototype ranging system estimation errors (m) measured relative to the GPS range estimate.

	sample no.	σ expected	RMS error	Min error	Max error
LOS	100	$\approx 1.9 + \sigma_n$	7.0	0.0	24.9
NLOS	100	$\approx 1.9 + \sigma_n$	15.8	0.0	79.5
Indoor	1000	$\approx 0.6 + \sigma_n$	1.7	0.3	3.2

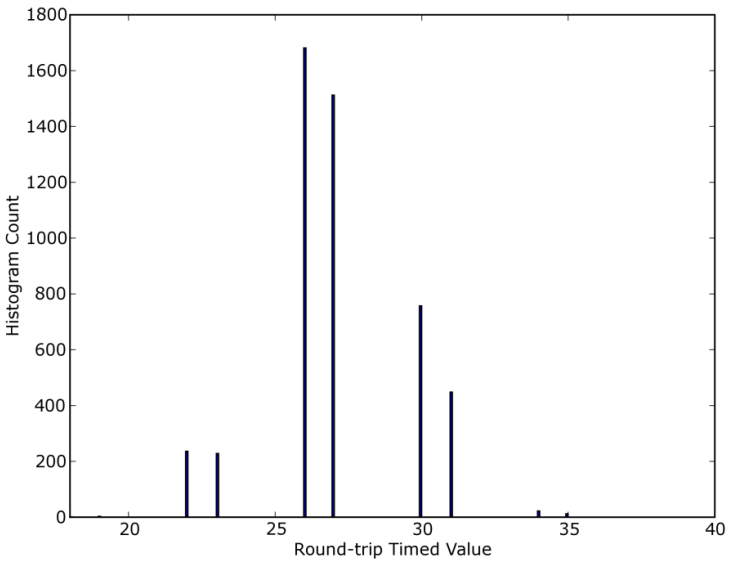


FIGURE 4.26: Histogram count of round-trip timed values for 5000 two-way TOA measurements using the TI CC2430.

at best, resolution is 18.75 m (two-way ranging). Averaging 100 round-trip estimates for outdoor LOS and NLOS conditions has demonstrated ranging accuracies of 7.0 m RMS and 15.8 m RMS. Indoor conditions with 1000 round-trip estimates has demonstrated ranging accuracy better than 1.7 m RMS, those results compare well with the expected accuracies for the sample size and it is expected that further improvement can be made by more accurately generating the frequency difference between the transceivers involved with ranging.

In comparison to UWB-based TOF ranging systems that are intended for precise ranging [13, 21], the results do not compare well (accuracies < 2.0 m in comparison to accuracies < 0.5m for UWB TOF ranging). The UWB locating system presented in [21] utilises a TOA range measurement system with a one-nanosecond resolution (0.3 m) through the use of a tapped delay line and FPGA-based comparator. Although this system utilises a TDOA architecture for timing synchronization, it is expected that the timing techniques and use of UWB signals could be adopted to a two-way ranging system similar to that presented in this work. The key differences are edge-detection versus time duration for estimation of the precise arrival of a ranging signal and the signal bandwidth used. The effects of those parameters are detailed in chapter 3 along with

their limitations. It is expected that the prototype ranging algorithm herein could meet similar accuracy to that of the mentioned UWB-based ranging system. This may be achieved through further modification to the generation of the frequency difference between the transceivers involved with the ranging process as detailed in this chapter.

Chapter 5

Prototype Locating System

In this chapter a two-dimensional localization system based on the use of RF ranging is presented that operates with relaxed synchronization requirements and no wired connectivity between references to alleviate the constraints of alternative localization systems. The use of narrow-band RF signals also allows operational range within regulation over much greater distance ($>$ 100 m) than alternative UWB-based locating systems described in chapter 1. The RF TOF ranging system with phase offset measurement presented in the previous chapter is utilised in order to develop a position estimation algorithm to locate and track a blind device within the requirements of WSNs. Resolution of 0.3 m and accuracy of better than $\pm$1.0 m for LOS conditions and $\pm$2.5 m for NLOS conditions (for 50% of estimates) is typically required. A sensing device with no prior knowledge of its position ('blind' device) can be located or tracked either by triangulation or trilateration [62, 41, 78]. The focus is on trilateration using the developed RF TOF ranging method. Trilateration or 'multilateration' involves the position computation through the measurement of the range (distance) of the blind device to or from a set of references. An accepted problem with locating is the ability to accurately estimate the position of a blind device in the presence of noise, NLOS signal propagation and signal multipath [13, 64, 79]. Commercialized asset locating systems such as the PAL650 asset locating system by Multispectral Solutions [21] have utilised TOF ranging and Ultra-wideband transmission signals (bandwidth $>$ 500 MHz) to mitigate the effects of those error sources and enable precise position estimation accuracy (accuracy $<$ 0.5 m) of 'tags' in complex indoor environments. Position estimation variance is reported below (0.10,0.50)m in the x-y axis using a David-Fletcher-Powell minimization algorithm to compute a three-dimensional position estimate [21]. The use of UWB ranging signals however limits the operational range of the system because of regulation on transmission power of such wideband signals. For this reason, UWB systems are more suited for short range ($<$60 m), indoor applications. In addition, the requirement of wired infrastructure between referencing architecture to meet the timing synchronization requirements of the Time-Difference-Of-Arrival (TDOA) based system is a costly overhead and limits the

application of those systems.

Received signal strength indication (RSSI) is the most widely used ranging method for localization in WSNs because of its simplicity. However, RSSI based locating systems are reported to be less suitable for accurate localization in cluttered indoor environments because of the limited accuracy, poor resilience to signal multipath and complex models required to correct for errors [25]. This work aims to alleviate the constraints of alternative locating systems including RSSI measurement, Ultra-wideband transmission bandwidth, wired infrastructure between referencing architecture and the dependence on system clock frequency for high resolution. RF TOF ranging is employed with phase offset measurement. This involves measuring two-way ranging transactions between an blind device to be located (initiator) and several reference devices at known locations (responders) to enable the following novel aspects of the locating system:

- Relaxed synchronization using low-frequency drifting system clocks (32 MHz) removing the requirement of wired infrastructure between referencing architecture.
- Narrow-band TOF ranging using standard IEEE 802.15.4 radio transceivers enabling operational range within regulation over greater distance (>100 m) as required for WSNs in comparison to alternative UWB based locating systems.
- Aim of meeting position estimation and tracking ability with resolution below 0.3 m and accuracy better than ±1.0 m for LOS conditions and ±2.5m for NLOS conditions (for 50% of estimates).

The localization system herein also aims to meet the requirements of the diverse range of WSN applications by using standard off-the-shelf WSN hardware. This method of locating and tracking blind devices within WSNs is expected to be more cost effective and or power efficient than alternative UWB-based or acoustic locating systems. This is because ranging could be performed in conjunction with data transfer and there is no requirement of wired infrustructure or high frequency system clocks. Furthermore, algorithms have been developed to operate in coexistence with current hardware and wireless protocol standards with no additional overheads. Prototyping and development has been carried out using a TI CC2431 development kit [20]. Ranging and data packet transfer is carried out on a single 2435MHz channel in the 2.4GHz industrial, scientific and medical (ISM) band. The system is compliant with the IEEE 802.15.4 standard and may be adapted to operate in other subsequent wireless standards such as IEEE 802.11.

5.1 Summary of Locating Systems and key parameters

There are a number of localization systems in the literature based on the use of time-of-flight (TOF), time-difference-of-arrival (TDOA), received-signal-strength-indication

(RSSI), near-field-electromagnetic-ranging (NFER) and angle-of-arrival (AOA) ranging or localization techniques. The key distinctions between those systems include power consumption, system clock frequency, hardware requirements, synchronization requirements, resolution, accuracy, signal bandwidth and the ranging technique(s) utilised.

Table 5.1 summarizes the key parameters for five locating systems including the TI CC2431 locating engine, Ubisense, PAL-650, Crossbow criket, Q-track NFER system and the prototyped RF TOF locating system herein. The circular error probable (CEP) is commonly used to describe the performance of those systems and defines a circular area centred around the mean position estimate that 50% of position estimates are within for a given true position. It can be seen that precise locating systems utilise wideband signals (bandwidth >500 MHz) to achieve a circular error probable (CEP) of 0.3 m. However, as mentioned previously, Ultra-wideband signal bandwidth limits the operational range. One alternative locating system by Q-track utilises NFER and IEEE 802.15.4 radios for data communication to enable position estimation accuracy of <1.0 m. However, the use of the AM broadcast band (530-1710 kHz) means that this system can interfere with other systems operating within the AM frequency band and therefore the Federal Communications Commission (FCC) limit the maximum transmission power of NFER based locating systems thus also limiting the operational range.

The developed RF TOF locating system herein has been prototyped on the TI CC2431 development kit however other subsequent hardware platforms may be used. In comparison to the RSSI based z-location engine employed on the TI CC2431, it is expected that RF TOF ranging will enable greater position estimation accuracy and improved reliability of position estimates without the requirement of complex models to correct for errors associated with RSSI based ranging. To evaluate the prototype RF TOF locating system, comparison with RSSI based locating results obtained using the TI CC2431 z-location engine is carried out. Similar configuration parameters are used for experimental results including transmission power, system clock frequency, resolution and accuracy in order to illustrate that RF TOF ranging is an alternative technique for localization within WSNs to meet the accuracy and resolution requirements of those systems.

5.2 Position Estimation Problem

The problem of locating a blind device in two-dimensions is illustrated graphically by the intersection of ranging rings as shown in figure 5.1. The number of ranging measurements required to each independent reference Ref_i is bound by the number of degrees of freedom (i.e. the number of co-ordinate axis). Ranging to a single reference Ref_1

TABLE 5.1: Key parameters of available locating systems.

	TI CC2431 locating engine [20]	Prototype RF TOF locating engine	Ubisense [22, 68]	PAL-650 [21]	Q-track [59]	Crossbow Cricket [80]
System clock frequency	32 MHz	32 MHz	-	100 MHz	-	8 MHz
Synchronization requirements	No	No	Yes	Yes	No	Yes
Transmit power (typical)	700mW	700mW	-	30mW	100mW	-
Wire infrastructure requirement	No	No	Yes	Yes	No	No
Deployment area (maximum)	64 m^2	250 m^2	1000 m^2	164 m^2	930 m^2	-
Resolution	0.25 m	Δt	0.05 m	0.3m	0.3 m	0.01 m
Accuracy	<3.0 m	0.5 m CEP	0.3 m CEP	0.3 m CEP	<1.0 m	0.01 m
Signal bandwidth / Operating frequency	2 MHz / 2.4 GHz	2 MHz / 2.4 GHz	500 MHz / -	1.25 GHz / 6.2 GHz	500 MHz / 575 kHz - 1700 kHz (data link 2 MHz)	- / 433 MHz data link
Ranging technique(s)	RSSI	RF-TOF	TDOA/AOA	TDOA	NFER	Accoustic-TOF

places the blind device on a ring with radius r_1 centred about reference r_1. A second range measurement to a reference Ref_2 positions the blind device at either intersect of two ranging rings. To resolve this ambiguity, a third range measurement r_3 is made to reference Ref_3. Thus, a minimum of three reference devices must have a direct LOS or at most an attenuated LOS transmission path to accurately determine the position of a blind device with no ambiguity in two dimensions. In the case of a three-dimensional position estimation problem, the blind device position is estimated by the intersection of spheres, where a minimum of four ranging measurements must be performed to remove the ambiguity resulting from the third degree of freedom [18]. In the presence of noise and NLOS signal propagation, range measurements have independent errors which are represented in figure 5.1 by variances $\sigma_{\epsilon(1)}, \sigma_{\epsilon(2)}, \sigma_{\epsilon(3)}$. Ranging rings therefore have widths dependent on the ranging error variance and no longer intersect at the blind devices true position P_0. For this reason, the blind device is said to be within a triangular error space represented in figure 5.1 by the shaded region ABC.

Ambiguity and NLOS Signal Propagation

A key problem in accurately locating a blind device is the effects of signal multipath and NLOS propagation. There are many algorithms in the literature which attempt to mitigate those errors by distinguishing LOS and NLOS measurements [73], [64], [81]. In [73] it is reported that NLOS measurements have greater variance than LOS measurements, confirming the findings of the research in the proceeding chapter. It has also been reported in [64] that using pure statistical characteristics to distinguish NLOS measurements from LOS measurements is a difficult problem. In circumstances of large range errors (i.e. indoor NLOS environment up to 50%), ambiguity can result in the position computation of the blind device if a position estimate is computed using more

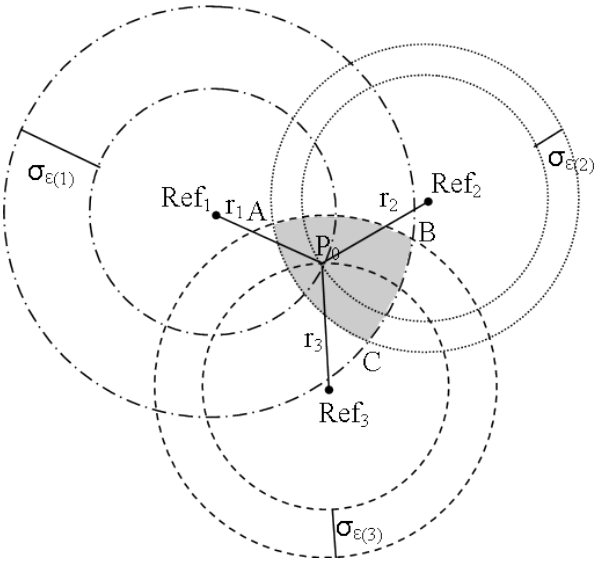
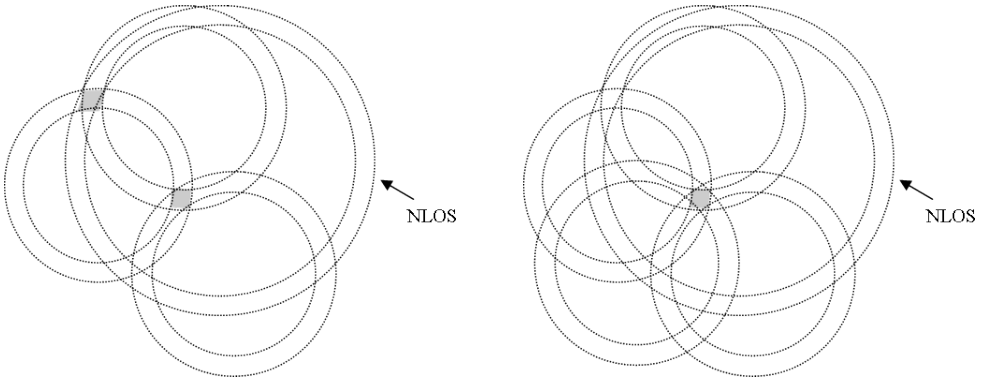


FIGURE 5.1: Position estimation of a blind device P_0 in two-dimensions by the intersection of ranging rings from three independent references Ref_1 - Ref_3 with ranging errors $\sigma_{\epsilon(1)}$ - $\sigma_{\epsilon(3)}$. Blind device is located within triangular error space ABC.

than the required number of range measurements. More than one valid solution may exist for the position estimate of the blind device. The ambiguity caused by multipath, NLOS propagation and over-determined solutions can be resolved as shown by figures 5.2(a) and 5.2(b). Figure 5.2(a) illustrates the case where four range estimates produce two solutions to the position estimate when one ranging measurement inherits significant error from noise or NLOS signal propagation. Figure 5.2(b) illustrates how five range estimates is used to resolve this problem. Hence an algorithm is required to remove ambiguity caused by noise and NLOS signal propagation. In cases where multiple solutions occur, this implies that one or more of the range estimates are NLOS. If N estimates are NLOS then at least N+1 (N>3) LOS estimates are needed to obtain an unambiguous position estimate [64]. This indicates that if more than three references are available, the performance of position estimation can be improved significantly in the presence of sever ranging error. However, position estimation accuracy can be better or worse than ranging accuracy depending on the geometry of the blind device in relation to references and the position estimation algorithm employed in the system.

Geometry and Dilution of Precision

Dilution of Precision (DOP) is the effect of transferring ranging errors to the position estimate in two or three dimensions [18]. In the presence of range measurement error, the computed two or three-dimensional position will inherit error which is dependent on the positions of the blind device and reference nodes relative geometry. If the angle between two references and the blind device are at right-angles, the position computation of the blind device will inherit small error. If the angle between the equivalent two references and the blind device is small, the position computation of the blind node will inherit larger error. Hence DOP represents the amplification of the standard deviation of range



(a) Example of position estimation ambiguity with 3 LOS and 1 NLOS range estimates. There are two valid position estimates for the blind device hence ambiguity exists [64].

(b) Ambiguity resolved by 4 LOS and 1 NLOS ranges estimates [64].

FIGURE 5.2: Resolving position ambiguity by N+1 range measurements.

measurement errors onto the position estimate of the blind device. The measure is represented by equations 5.1-5.3 in terms of position DOP (PDOP) , horizontal (HDOP) and vertical (VDOP) , where σ_{xb}, σ_{yb} and σ_{zb} are the percentage range variances in the x-y-z directions respectively. The effect of DOP on position estimation is shown in figure 5.3 using our developed position estimation algorithm in simulate mode. Position estimates towards the centre of the test area inherit less variance. In contrast, the variance increases towards the edges. Note that this simulated model does not include effects of multipath or NLOS signal propagation which may result from obstacles within the test area. Variance in range measurements can be used to calculate a locating systems inability to accurately locate a blind device.

$$Position\ Dilution\ of\ Precision\ (PDOP) = \sqrt{\sigma_{xb}^2 + \sigma_{yb}^2 + \sigma_{zb}^2} \quad (5.1)$$

$$Horizontal\ Dilution\ of\ Precision\ (HDOP) = \sqrt{\sigma_{xb}^2 + \sigma_{yb}^2} \quad (5.2)$$

$$Vertical\ Dilution\ of\ Precision\ (VDOP) = \sigma_{zb} \quad (5.3)$$

5.3 System Implementation

5.3.1 Position Estimation Algorithm

Sensor nodes are resource constrained with respect to hardware and processing power. In addition, the constraints of wireless sensor nodes having to operate from single battery sources implies processing duty cycle must be kept to a minimum. From a localization perspective, the algorithm enabling a sensor node to estimate its position must also be

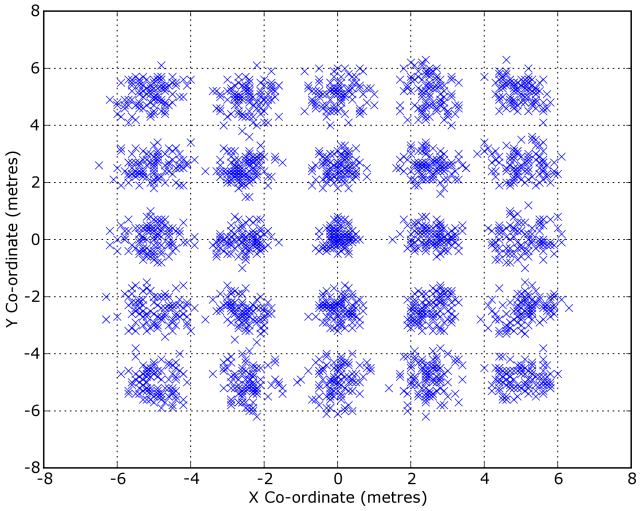


FIGURE 5.3: Simulated position estimation with effects of dilution of precision (DOP). Testing 2.5 m grid intersects over 5.0 m x 5.0 m area. Position estimation resolution 0.1 m, ranging measurement variance $\sigma = 0.7$ m. Simulated model does not include effects of multipath or NLOS signal propagation.

adaptable to the constraints of sensor nodes including simplicity, low energy consumption and scalability since WSNs can consist of hundreds of sensor nodes which may operate with either single-hop or multi-hop communication protocol. The algorithm must also be able to tolerate large range estimate errors (up to 50% of the range) which are expected in high multipath environments. There is a wide variety of techniques that can be employed for position estimation. In this work a simple 'brute-force' method using a grid search over a specified test area is used. Development of this method would adapt an optimizer to reduce the computational time of obtaining a position estimate. Previous research has show optimization methods for position estimation function well [21]. In addition, they are closely suited to the constraints of sensor nodes including simplicity, low processing overheads and fast computational time enabling low duty cycle. The position estimation problem is considered as a cost function that needs to be minimized. A position estimate is computed for a number of test positions, where the test position with the least error is approximated as the position estimate of the blind device. Testing is carried out using a grid system for the x-y positions defined by the user with respect to the references. Thus, the resolution of this algorithm is bound by the size of grid squares (δ_{xy}). The position error ϵ_{xy} in three-dimensions is defined by equation 5.6 by subtracting the calculated range-sum (d_i) from the estimated range-sum ($\hat{P}_{ei}$) described by equations 5.4 and 5.5, where the blind device test position has co-ordinates (x_t, y_t) and the i^{th} reference has co-ordinates (x_i, y_i) for each test position. The algorithm used a a square-sum error criterion, where the cost function is represented by equation 5.7. This is just the sum of the squares of the errors. Those are placed into an n-dimensional array with dimensions corresponding to the co-ordinate axis. The minimum error is located and the corresponding x-y co-ordinates of the blind device are found. Large

errors in position estimates caused by multipath propagation under NLOS conditions are reduced by averaging a sample of n estimates per position estimate.

$$d_i = \sum_{i=1}^{n} \sqrt{(x_i - x_t)^2 + (y_i - y_t)^2} \tag{5.4}$$

$$\hat{P}_{ei}(E) = \sum_{i=1}^{n} r_i \tag{5.5}$$

$$\epsilon_{xy} = \hat{P}_{ei}(E) - d_i \tag{5.6}$$

$$C(\epsilon_{xy}) = (\hat{P}_{ei}(E) - d_i)^2 \tag{5.7}$$

The prototype position estimation algorithm is demanding in terms of the number of iterations and processing time, however, both of those overheads can be reduced by implementation of an optimizer to find the minimum cost of 5.7. For simplicity, a brute force search is used in order to find the local minimum and averaging to reduce or remove error caused by NLOS signal propagation. Using the brute force approach, the system typically computes a position estimate approximately every two seconds using a 0.1 m resolution search grid. This is expected to be suitably fast for WSN applications where position refresh rates can be in the order of once per minute to once per month. To remove any position ambiguity in the blind device computation and the effects or NLOS signal propagation, multiple TOA measurements and over-determined position estimation algorithm are used to mitigate the effect of error from NLOS signal propagation. In addition, the system relies on the high accuracy TOF ranging scheme and its DSSS modulation to reduce those errors.

5.3.2 System Description

The system consists of a set of 'blind' devices to be located relative to a set of references, which have a prior knowledge of their position with respect to a two or three-dimensional co-ordinate system. Those are distinctly separated in both the horizontal axis and vertical axis around the perimeter of the area to be monitored. Range estimates are initiated by the blind device but could subsequently be initiated by the referencing architecture if additional time allocation algorithms where incorporated to enable this technique. A controller device and laptop computer are interfaced by wired RS232 connection and used for the control, position computation and display of the estimated position of the blind device in question. Blind devices have no prior knowledge of their positions and perform ranging to each of the four available references. Ranging data is broadcast by the blind device to a controller to enable computation and graphical display of the blind device positions via a laptop computer. Position estimation is computed in two dimensions by solving the cost function described by equation 5.7. This method

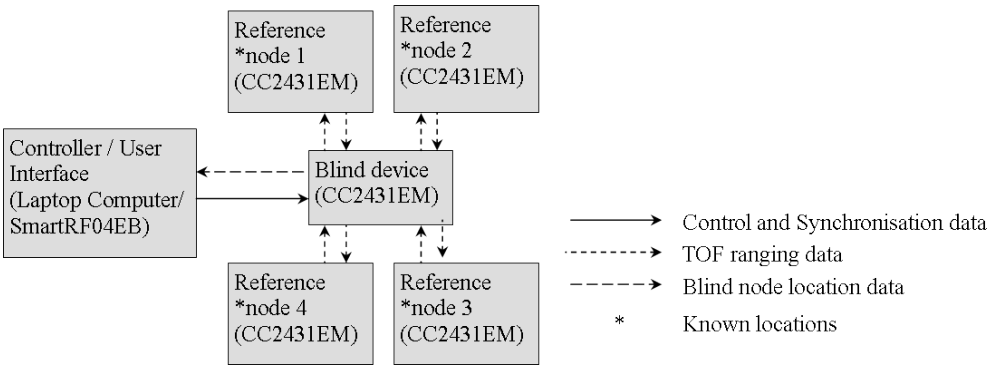


FIGURE 5.4: Block diagram of prototype locating system architecture. Hardware consists of five TI CC2431EM (four references and a single blind device) and one TI SmartRF04EB interfaced to a laptop computer via RS232.

is computationally simple and can be extended to compute position estimates in three-dimensions. Graphical representation of the position estimate is displayed in relation to the referencing architecture via a laptop computer. The positions of reference devices are assumed precise and the calibration of range measurements are assumed preset within the ranging algorithm, thus a start-up calibration phase is not performed by the locating system algorithm.

A TI CC2431 development kit has been used to prototype the locating system [20]. Aside of the RSSI-based locating engine, the TI CC2431 is identical to the TI CC2430. The physical size of hardware is mainly constrained by the development platform for the TI CC2431, however the TI CC2431 I.C. is 8 mm x 8 mm in size and hence the physical size of references, blind device tags and the user interface can be significantly reduced in a manufactured system. The setup of hardware is illustrated from the block perspective in figure 5.4. Each system component operates independently from its own battery source (either a PP3 or two AA batteries) and there is no wired infrastructure between the references for timing synchronization or data transfer. Each independent reference (Ref_i) has co-ordinates (x_i,y_i) and is assigned a unique one-byte address (Add_i) such that ranging may be performed from the blind device to each reference independently in a periodic manor. To mitigate the possibility of ranging and data packet collision when multiple blind devices are used, time allocation slots may be provided by the controller device. Ranging packets have been left unmodified from the previous work and are 11 bytes in length. Subsequently, data packets for the transfer of ranging data to the controller are 17 bytes in length. Those contain the blind devices address and each ranging measurement with its corresponding reference address and are configured in compliance with IEEE 802.15.4 protocol. A clear-to-send check is made before the transmission of packets, however, if ranging or data packets become corrupt or lost, the position estimation is disregarded.

5.3.3 Software Overview

There are five software algorithms associated with the based prototype RF TOF locating system. Those include reference nodes, co-ordinator, graphic user interface, position estimation algorithm and blind device. The reference nodes simply reflect ranging packets that are addressed specifically to the reference node in question. This software process is detailed in the previous chapter and remains unmodified. The co-ordinator, graphic user interface and position estimation algorithm are linked together through Python software and a simple algorithm programmed on to a TI CC2430 development board to enable receive and transmit of data packets and the control of the locating system via an RS232 interface to the laptop computer. The position estimation algorithm simply performs the function detailed by equations 5.4 - 5.7 and displays each position estimate within the test area via Python and TKinter software. Blind devices follow the software procedure as follows. The device is initialized and the locating process is activated. A ranging data packet is created following range measurements to each reference device. The ranging packet begins with 'identifier' and 'address' bytes to enable the co-ordinator to identify the packet type and the address of the device which has transmitted this data. Range measurements are performed to each reference node in turn with address 'nodeAddress' using the function tofRange(nodeAddress) which performs the RF TOF ranging function decribed in the previous chapter. The ranging data is added to the ranging data packet in specific order with its corresponding reference node address. Once range measurements have been obtained to all of the available reference nodes, the ranging data packet is broadcast to the locating system co-ordinator enabling the position of the blind device to be estimated and displayed graphically. A high level software overview is illustrated below for an independent blind device. Further development to the system will include the time allocation slots enabling a locating system with much greater numbers of blind devices.

```
if(radio_initialization == true)
  {
  while(locating_process == true)
     {

      ranging_data[0] = 0xAB;  // identifier
      ranging_data[1] = 0xAC;  // address

  //Range to Reference with address 01
      nodeAddress = 01;
      ranging_data[2] = nodeAddress;
      ranging_data[3] = tofRange(nodeAddress);

  //Range to Reference with address 02
      nodeAddress = 02;
      ranging_data[4] = nodeAddress;
      ranging_data[5] = tofRange(nodeAddress);

  //Range to Reference with address 03
      nodeAddress = 03;
      ranging_data[6] = nodeAddress;
      ranging_data[7] = tofRange(nodeAddress);

  //Range to Reference with address 04
      nodeAddress = 04;
      ranging_data[8] = nodeAddress;
      ranging_data[9] = tofRange(nodeAddress);

     pointer = ranging_data;
     length = 10;
     count = SendPacket(pointer, length);

     }
  else
     {
      lcdUpdate('Config_Failure','');
      return 0;
     }
  }
```

Experimental setup

Testing is performed and evaluated for a single blind device where ranging is performed to four references with prior knowledge of their positions. The fundamental localization system may then be extended to include a larger number of 'blind' devices by the use of a method such as allocated time slots for the localization of each device in question. The TI CC2431 development kit platforms remain unmodified with software algorithms developed in C and flash programmed on to each hardware platform independently. Each reference is assigned a unique address during programming in order that range measurements are performed to the correct reference. In contrast, the position estimation algorithm is prototyped in Python software. The area bound by the perimeter formed by references is divided up into grid squares. The resolution of the gridded area is preset in software to give the desired locating resolution. Grid squares have unique x-y

co-ordinates relative to the reference positions and are used to compute the estimate-position-sum. Those values are then subtracted from the range-estimate-sum and each error is recorded for the test position with unique x-y co-ordinates. Error values are then scaled and assigned a colour ranging from blue to red, where warmer colours represent closer approximations of the blind devices true position. The grid test area and assigned colours are displayed graphically via TKinter on a laptop computer. Reference positions are represented by black circles, the approximate position of the blind device (i.e. the position with least error) is boxed and the corresponding co-ordinates are recorded. The locating system latency including update of the user display is approximately 2 s when a 0.1 m resolution is used. Figure 5.5 illustrates a screen shot of prototype locating system graphical user display. IPython Shell window illustrates output data strings of three independent position estimates. The first line contains the estimated x-position, y-position, z-position estimates and maximum, minimum position estimate errors. Maximum and minimum position estimate error are calculated based on equation (5.7) and scaled accordingly to represent position error as a percentage error. The algorithm is configured to estimate position in two-dimensions but can be extended to operate in three-dimensions by including the 'z' term in equation 5.4. The second line encapsulated by quotations illustrates a data packet as received by the Python program where each data value is separated by a comma. The first number is a predefined, arbitrarily chosen integer used as a data packet identifier, in this case 18. The proceeding two data values of 255 are included to enable further development of the locating system but are redundant for experimental testing. Each reference node address followed by its corresponding range measurement by the blind device is then included in the order of references with pre-defined integer addresses 64, 48, 39, 83 which are arbitrary chosen. Proceeding bytes within the data packet are redundant in the prototype locating system. The third to sixth lines show each node address and corresponding range estimates in metres. Finally if the ranging data has been successfully obtained (i.e. range estimates to each of the four references) then an acknowledgement message "complete ranging data" is displayed else the data set is disregarded. The position estimation procedure is re-computed each time a valid set of ranging data is received by the Python software. The TK inter window illustrates the position estimate of the blind device (white outlined square) in relation to the set of reference positions illustrated by black circles. Each square of the gridded area represents the error in the cost function for that particular location. Cold colours represent greater error in the position estimate in contrast to warm colours that represent closer approximation to the true position of the blind device. Thus, red indicates the locations with the least position estimate errors and hence the closest approximate of the blind devices position. The size of the grid squares is preset in software (resolution of algorithm) and in this illustration represents an area of 1.0 m^2 over a test area of 30.0 x 30.0 m^2. The latency of this algorithm may be significantly reduced by performing a course grid search followed by a refined search and optimizer to replace the current brute-force approach.

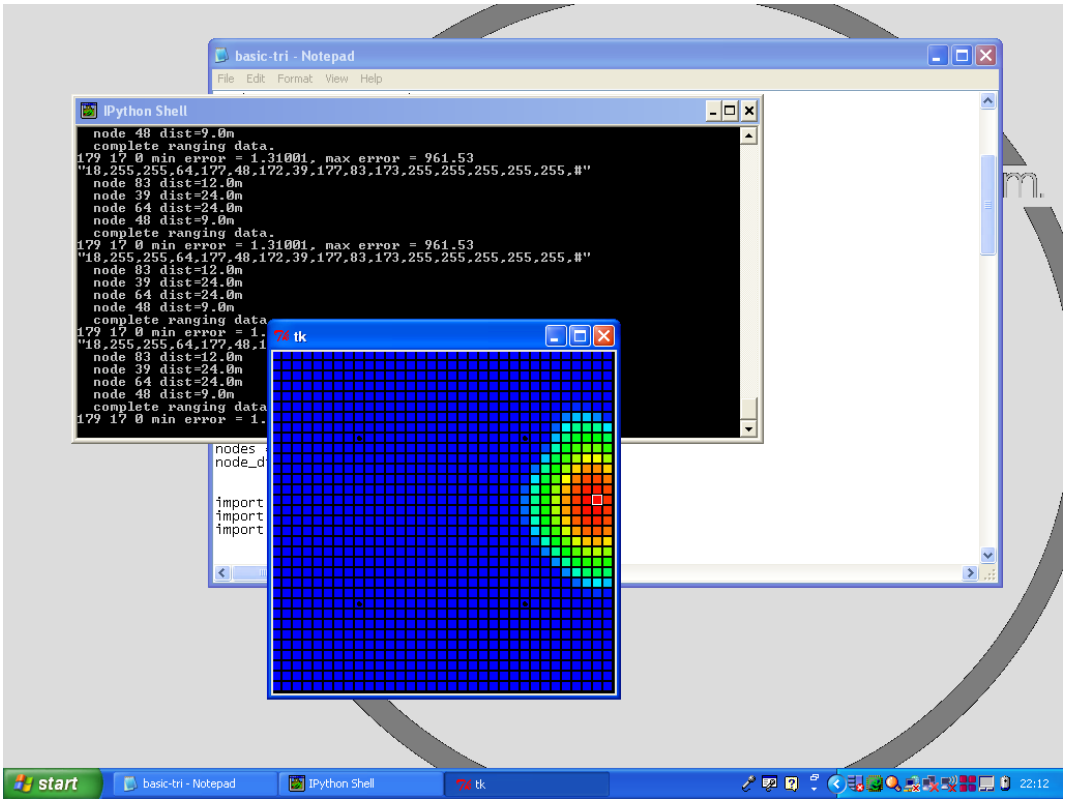


FIGURE 5.5: Screen shot of locating system graphical user display including IPython and TKinter windows.

5.4 Results

The prototype locating system has been tested for outdoor LOS and indoor NLOS environments using the standard TI CC2431 development kit operating on a single 2435 MHz channel with a transmission power of -1.5 dBm (700 uW). Testing for the non-obstructed LOS condition was carried out using four references placed 30.0 m apart in a square configuration to provide good geometric constellation. In contrast, indoor testing was performed in a residential flat constructed of brick and stud-partition internal walls. References were placed one metre above ground level on tripod stands in a rectangular 7.0 m x 3.5 m configuration restricted in size by room dimensions. The blind device was then placed on a similar tripod stand in several known test positions for evaluation of the locating system's performance. For both the LOS and indoor NLOS test areas, the position error between the true positions of the references and the actual positions of the references was expected to be between 0.0 - 0.3 m. This is because a tape measure was used to estimate the positions for the placement of references contributing a source of error. The objective of the testing was to determine how well the system would perform in locating the blind device for LOS and NLOS conditions using our prototype ranging algorithm. It was expected that walls and furnishings within indoor locating would make the estimation of position a challenging task. The testing procedure involved placing the blind device at known positions and recording the corresponding position estimate

multiple times. Any ambiguous or severely errored position estimates were not filtered or disregarded (i.e. estimates where one or more range measurements inherit error). The position estimation algorithm prototyped in Python software operates using a brute-force (fine grid search) approach with a pre-set resolution of 0.1 m. A combination of 20 ranging estimates per reference followed by 20 averaged position estimates was used to evaluate the performance of the system. Those parameters enable real-time tracking (2 s latency of estimates) with an expected variance of 2.0 m, assuming the absence of noise, multipath and a random clock offset during ranging. The absolute position accuracy is also dependent on precise knowledge of all the references positions. Figures 5.6 and 5.7 illustrate the performance of the locating system for the LOS condition where the blind device is positioned at (0.0,0.0)m. The mean estimate position was (-0.2,0.2)m with standard deviation 0.9 m in both the x-y-axis. The quantization of the histogram counts shown in figure 5.7 is due to the 0.1 m preset positioning algorithm resolution. Performance was consistent over the 30.0 m x 30.0 m test area with the error in position estimation expected through calibration error, noise and signal multipath.

Figures 5.8 and 5.9 illustrate the performance of the locating system for the indoor NLOS condition. Internal doors were left open during testing with references placed in different rooms as illustrated in figure 5.8. Rooms contained full furnishings including tables, chairs, bookshelves, glass units and many other surfaces which contribute towards signal attenuation and scattering. The blind device was placed at (-0.5,-0.5)m to provide a good signal attenuated position for the indoor NLOS test. The corresponding mean estimate position was (-1.2,-1.3)m with variance 1.4 m in the x-axis and 0.8 m in the y-axis. An increase in the estimation variance was expected under NLOS conditions with greater variance in the x-axis due to the geometry of the reference positions.

Table 5.2 summarizes the cummulative fraction of position estimates with error less than abscissa for 200 position estimates using our brute-force position estimation and RF TOF ranging algorithms. Position estimation accuracy is typically better than 2.00m for 98% of estimates outdoors under LOS conditions. Typical indoor position estimation accuracy is better than 3.00 m for 91% of estimates under NLOS conditions. Table 5.3 summarizes RSSI locating results obtained from the TI CC2431 z-location engine. Previous research agrees with the results presented in Table 5.3 where mean position estimate error is reported to be greater than 2.5m using two-dimensional position estimation for indoor LOS conditions with corresponding standard deviation of up to 2.19m [25]. References and the blind device are placed in the same geometric positions and environments as for our RF TOF based locating experiments. Our prototype RF TOF locating system performance results compare well with the TI CC2431 z-location engine using a 800 sample average (averaging 20 range estimates per reference followed by 20 position estimates).

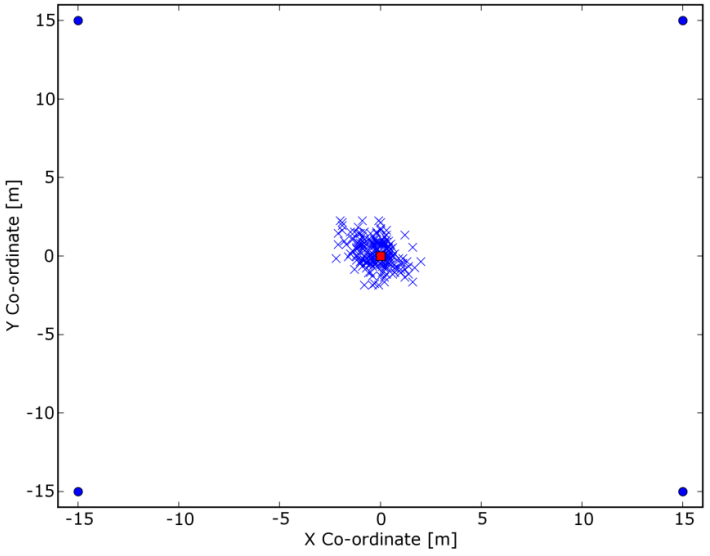


FIGURE 5.6: Performance of locating system for 30.0 m x 30.0 m area LOS outdoors. Blue-circles are reference positions, red-square is the true position of the blind device. 200 position estimates using 20 ranging samples per measurement and 20 averaged position estimates.

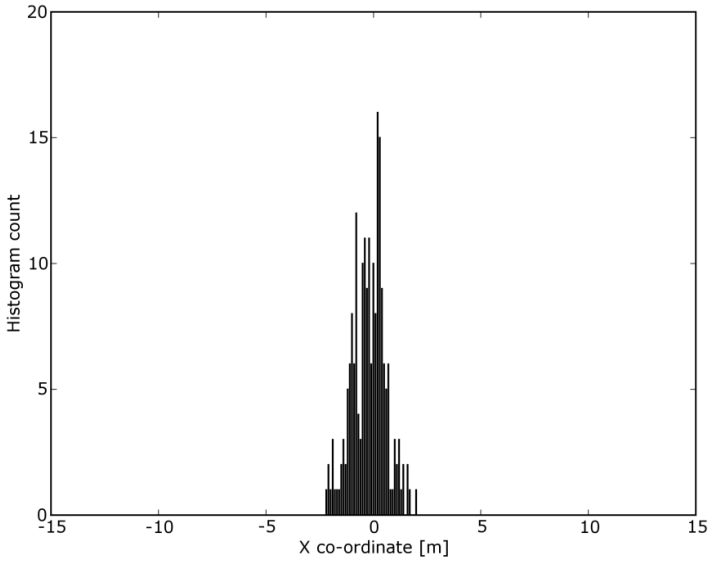


FIGURE 5.7: Histogram of collected x co-ordinate data, 200 position estimates for outdoor LOS condition (algorithm resolution 0.1 m).

Blind device position estimates using the z-location engine have consistent error between the blind device true position and the estimated position, typically between 0.0 - 2.0 m. We expect that complex models would be required to correct for those error discrepancies. Our prototype RF TOF locating system has demonstrated that although

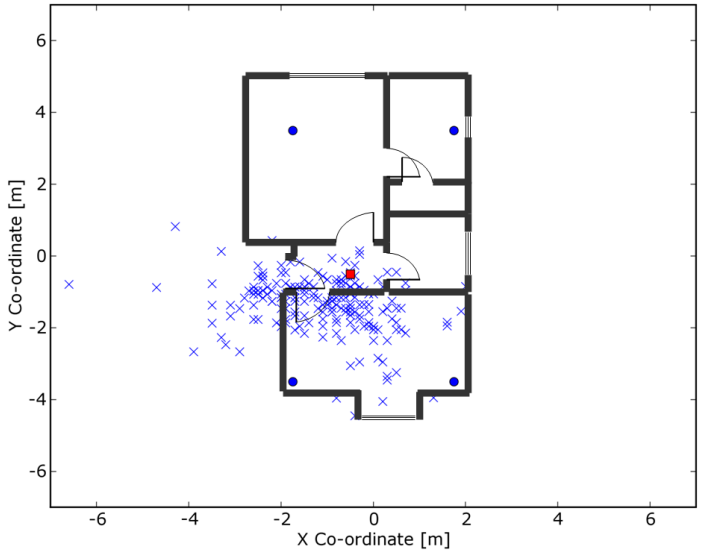


FIGURE 5.8: Performance of locating system for 7.0 m x 3.5 m area indoors. Blue-circles are reference positions, red-square is the true position of the blind device. 200 position estimates using 20 ranging samples per measurement and 20 averaged position estimates.

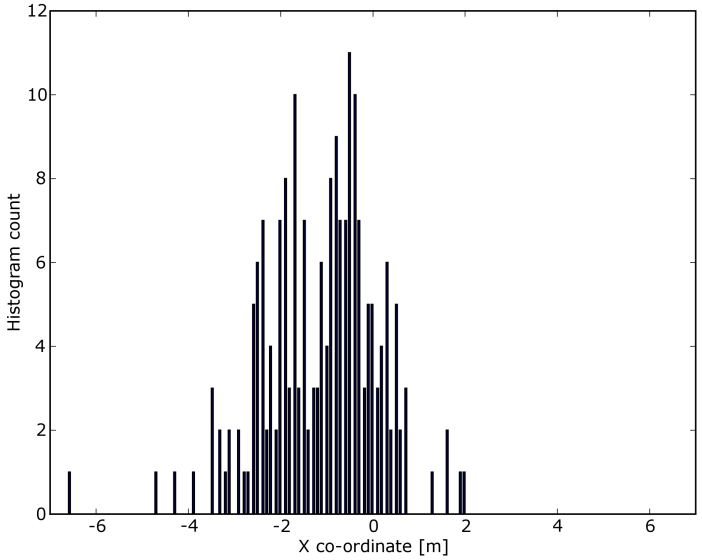


FIGURE 5.9: Histogram of collected x co-ordinate data, 200 position estimates for indoor NLOS condition (algorithm resolution 0.1 m).

variance in the current system is typically greater than that of RSSI based locating, position estimates more accurately correspond to the true position of the blind device in comparison. In addition, it has been noted that RSSI tracking does not perform as well as RF TOF tracking. When a blind device is moved from a known position and returned, RSSI position estimates do not remain consistent in comparison to RF TOF estimates that do.

TABLE 5.2: Cumulative fraction of readings with error less than abscissa for 200 x-y estimates for outdoor LOS and Indoor NLOS conditions.

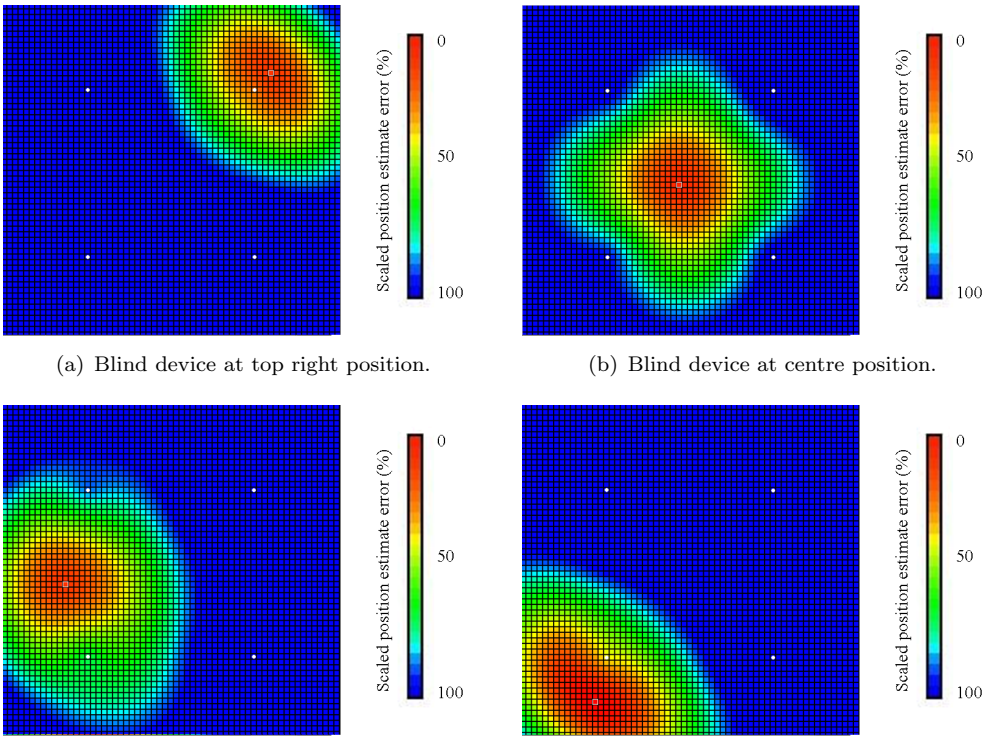
Error [m]	Outdoor LOS		Indoor NLOS	
	x	y	x	y
< 0.5	0.55	0.42	0.26	0.10
< 1.0	0.82	0.75	0.42	0.40
< 1.5	0.94	0.90	0.55	0.66
< 2.0	0.99	0.98	0.71	0.86
< 2.5	1.00	1.00	0.83	0.95
< 3.0	1.00	1.00	0.91	0.97
< 3.5	1.00	1.00	0.96	0.98
< 4.0	1.00	1.00	0.98	0.99
< 4.5	1.00	1.00	0.99	1.00
< 5.0	1.00	1.00	1.00	1.00

TABLE 5.3: Z-locating engine RSSI locating results for Outdoor LOS and Indoor NLOS conditions. True blind device positions, (15.0,15.0) outdoor LOS and (4.0,2.0) indoor NLOS.

Outdoor LOS		Error [m]		Indoor NLOS		Error [m]	
x	y	x	y	x	y	x	y
13.75	14.75	1.25	0.25	4.00	0.00	0.00	2.00
13.50	14.50	1.50	0.50	3.75	0.00	0.25	2.00
13.50	14.75	1.50	0.25	3.50	0.00	0.50	2.00
11.75	14.50	3.25	0.50	5.50	0.00	1.50	2.00
13.50	14.75	1.50	0.25	6.00	0.00	2.00	2.00
12.50	14.75	2.50	1.25	5.75	0.00	1.75	2.00
13.50	14.75	1.50	0.25	4.00	0.00	0.00	2.00
12.75	13.50	2.25	1.50	5.25	0.00	1.25	2.00
13.50	14.75	1.50	0.25	5.25	0.00	1.25	2.00
11.75	13.25	3.25	1.75	3.50	0.00	0.50	2.00

RSSI and TOF ranging both make use of the packet preamble sequence and SFD to estimate range. RSSI involves measurement of the received symbol periods amplitude in comparison to TOF that involves measurement of the phase shift of the symbol sequences. Thus, both techniques do not require additional hardware overheads in comparison to alternative ranging techniques. The performance of RSSI range estimates is improved by finding the average RSSI estimate over eight symbol periods (128 us). The performance of TOF estimates are similarly improved by averaging multiple round-trip transactions, we expect that this overhead could be significantly reduced by estimating the TOF period multiple times over the synchronization preamble sequence as with RSSI ranging, thus resulting in similar energy overheads. The accuracy of TOF estimates may also be quadratically improved by linearly increasing signal bandwidth enabling performance accuracy beyond the limits of RSSI ranging without the requirement of complex models to correct for errors.

The TI CC2431 incorporates the necessary hardware to perform TOF range estimates as



(a) Blind device at top right position.

(b) Blind device at centre position.

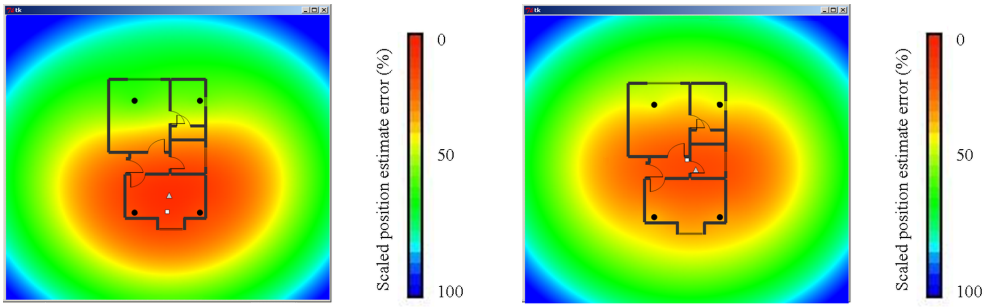
(c) Blind device at centre left position.

(d) Blind device at bottom left position outside test area.

FIGURE 5.10: Outdoor real-time position estimates using Python software algorithm.

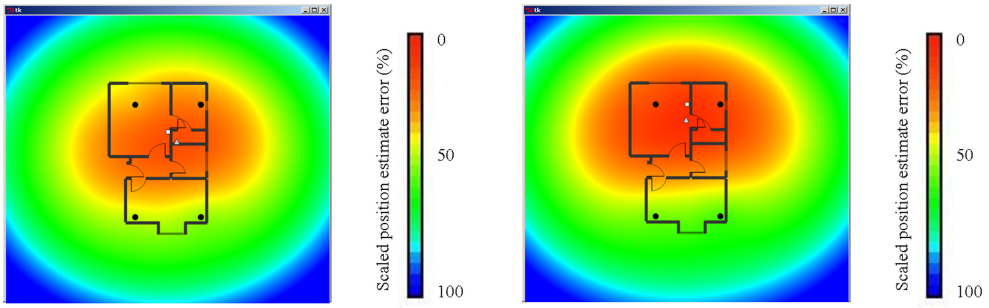
well as RSSI ranging. We expect that improvements to the hardware architecture could enable TOF ranging to be performed fully in hardware similar to RSSI ranging and thus reduce software overheads. However, RSSI range measurements require knowledge of the transmission power and only a single packet transaction in comparison to TOF ranging estimates that require the precise generation of Δt (the frequency difference between the initiator and responder) and a return signal transmission to enable the estimation of range. We expect that this process could be performed in conjunction with acknowledgement packets, thus reducing the additional overheads of this novel locating mechanism to those already available on the TI CC2431.

Figures 5.10 and 5.11 illustrate real-time screen shots of the locating systems performance as described in chapter 5 for a blind device in the said positions.



(a) Blind device at centre bottom position.

(b) Blind device at centre position.



(c) Blind device at positioned towards top middle.

(d) Blind device at centre top position.

FIGURE 5.11: Indoor real-time position estimates using Python software algorithm.

5.5 Summary

The following bullet points summarise the key aspects of this localization system:

- A two-dimensional localization system based on the use of narrow-band RF ranging has been presented that operates with relaxed synchronization requirements and no wired connectivity between references to alleviate the constraints of alternative localization systems.
- A key advantage of narrow-band RF signals is operational range within regulation over much greater distance (>100 m) than alternative UWB based localization systems.
- Localization resolution better than 0.3 m and accuracy of better than ±1.0 m for LOS conditions and ±2.5m for NLOS conditions (for 50% of estimates) is typically required for the specified application field.
- The work focuses on two-dimensional localization based on narrow-band RF TOF ranging using standard IEEE 802.15.4 radio transceivers enabling hardware specific for WSN applications to perform localization within the resolution and accuracy constrains posed.
- Performance results illustrate that this localization system has position estimation accuracy better than 2.00m for 98% of estimates outdoors under LOS conditions and position estimation accuracy better than 3.00 m for 91% of estimates under NLOS conditions.
- Performance results illustrate that this method of localization would be suitable for the specified wireless sensing applications including industrial, scientific and medical systems where sensor nodes are of low cost, standard with respect to hardware architecture, processing abilities and communicate using low-power narrow-band radios.

Chapter 6

Results Analysis

Chapters 4 and 5 describe prototype ranging and localization systems where parameters including resolution and accuracy are bound by the limitations described in chapter 3. Other limitations include power consumption, processing requirements, signal bandwidth and hardware overheads. Performance results of those prototype systems have been demonstrated. In this chapter, the results of the prototype ranging algorithm are analysed and simulation results are presented to illustrate the limitations of ranging performance illustrated in chapter 4. The performance of the ranging algorithm described in chapter 4 may be improved to meet resolution, accuracy and noise performance requirements of WSNs by the use of greater signal bandwidth and more precise system clock parameters and synchronization. This research demonstrates that narrow-band radios have the ability to meet the resolution and accuracy requirements for position estimation within WSNs as an alternative to UWB radios. Furthermore, because the accuracy and resolution of any locating system is fundamentally bound by the performance of the ranging technique utilised, ranging estimation performance is discussed in this chapter in terms of resolution, synchronization, noise performance and the effects of multipath and shadowing. Analysis is concluded by the implementation and demonstration of a filtering algorithm to illustrate that narrow-band ranging performance can be improved. The fundamental findings of this chapter are summarized as follows:

- Ranging accuracy is improved through multiple transactions up to the noise limit of the ranging system.
- The resolution of the ranging algorithm is bound by the function of the relative clock drift between the transceivers involved with the ranging process.
- The performance of the ranging algorithm is bound by four fundamental limitations including SNR, signal bandwidth, synchronization and the number of ranging transactions.

- The effects of noise, shadowing and signal multipath can be reduced by the use of filtering.

6.0.1 Resolution and Synchronization

Performance of the prototype ranging system is bound by the limitations explained in chapter 3. The resolution and accuracy of the system has been evaluated with the assumption that the relative phase offset between the initiator system clock and the responder system clock are normally distributed during the process of performing multiple ranging transactions. The distribution of raw round-trip measurements is shown in figure 4.26 and confirms this assumption, thus, averaging larger sets of round-trip measurements over a minimum of two time quantization bins enables improved TOF estimate accuracy. Figure 6.1 illustrates this to be the case by averaging sample sets of 100, 300 and 1000 round-trip measurements taken over a distance of 100.0 m LOS to provide a clean set of range estimates and minimize error contribution from multipath and shadowing effects. Ranging estimates deviate less from the true distance, thus variance is reduced by increased sample numbers. However, the linearity of range estimates does not fall within the accuracy constraint of just over 1.0 m as expected for a sample number of 1000. This non-linearity of range estimation is confirmed in figure 6.2. A sample set of 1000 range estimates are determined independently at 1.0 m increments over a distance of 0.0 m - 13.0 m. Testing is performed at two independent environments to remove ambiguities caused by multipath and shadowing. The non-linear relationship remains unchanged indicating that its function is a result of the radio transceiver hardware (i.e. inaccurate assumption that the relative clock phase offset between the initiator and responder is a random function). Figures 6.3(a) - 6.3(d) illustrate raw round-trip histograms for ranging distances 4.0 m, 6.0 m, 8.0 m and 10.0 m with LOS conditions using 1000 samples per estimate. The distribution of round-trip measurements shift from left to right with increasing initiator-responder distance as expected. However, the corresponding time period distribution is not consistent (i.e. normal) with increasing initiator-responder distance therefore contributing error to TOF estimates. An expected complex function therefore exists from three error sources including: the relative phase offset function between initiator and responder clocks (synchronization); delay from transceiver signal lock time; noise sources within the radio.

Error in sub-clock phase measurement is a result of the unknown function of relative clock phase between the initiator and responder. The TI CC2430 correlates received chip sequences at 8 MHz. The resolution of a single ranging transaction is thus bound to 37.5 m (d = ct = c/8 MHz). Round-trip timing resolution is 31.25 ns (32 MHz) thus when multiple range estimates are averaged in the presence of noise and transceiver clock drift, as absolute ranging resolution of 9.4 m is obtainable. As two-way ranging is employed, absolute ranging resolution is 4.7 m (9.4 m/2). However, in the presence of noise and

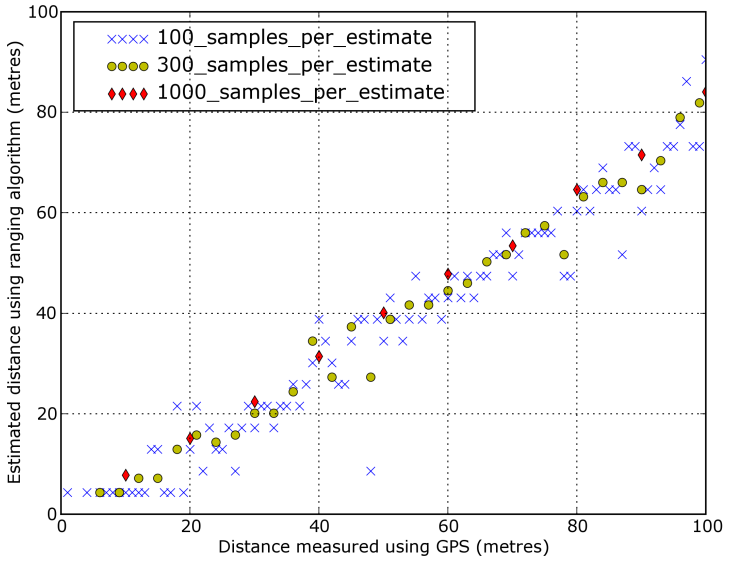


FIGURE 6.1: Effect of averaging on ranging performance for the LOS condition. Range estimation using 100, 300 and 1000 two-way ranging transactions.

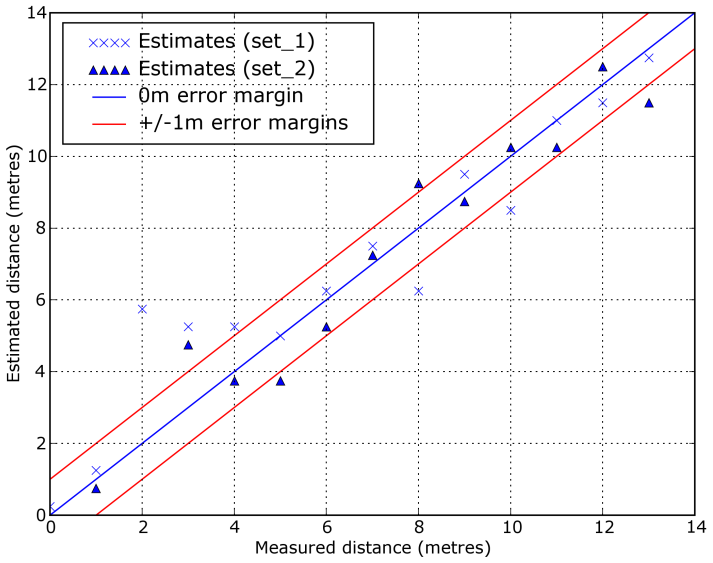
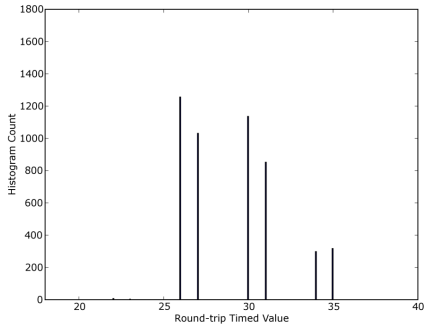
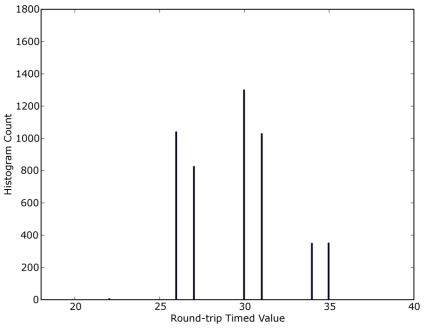


FIGURE 6.2: Non-linear characteristic of TOF ranging over range 0.0 m - 13.0 m in one metre increments.

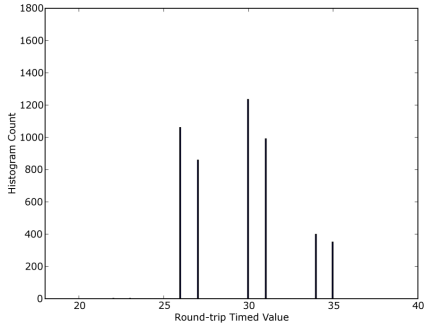
transceiver clock drift, this is a lower bound theoretical estimate of ranging resolution. The function of the relative clock phase between the initiator (A) and responder (B) utilised for sub-clock phase measurement can be categorised by three cases: 1) A and B have synchronized clocks; 2) a frequency difference Δt exists between A and B; 3) A and B have similar clocks which have normal or uniformly offset phase. The effect of each case on sub-clock phase estimation is best explained using the model illustrated in figure 6.4. Independent ranging transactions are detected in the nth bin according to the phase



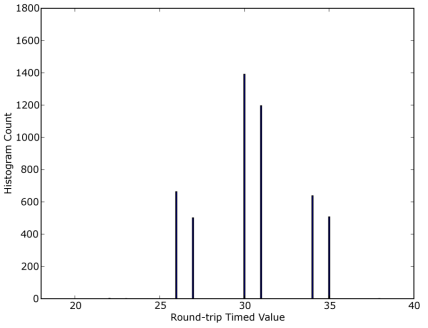
(a) Initiator-responder separation: 4.0 m.



(b) Initiator-responder separation: 6.0 m.



(c) Initiator-responder separation: 8.0 m.



(d) Initiator-responder separation: 10.0 m.

FIGURE 6.3: Distribution of 3000 two-way TOA range measurements for outdoor LOS condition for 4.0 m,6.0 m,8.0 m and 10.0 m initiator-responder separation distance. Raw distribution of round-trip timed measurements is not consistent with distance.

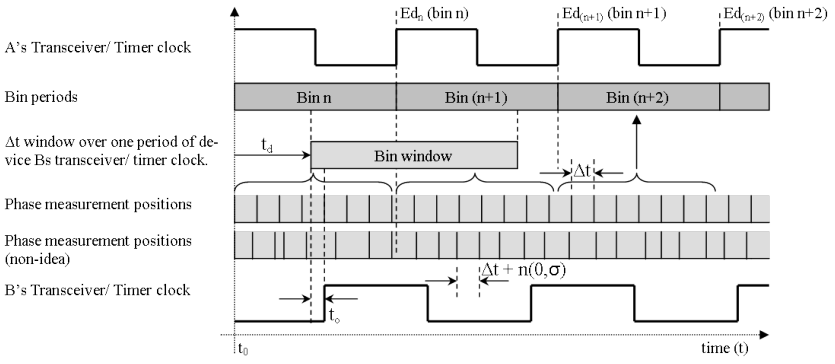


FIGURE 6.4: Simplified model implemented in Python software to illustrate TOF phase measurement techniques in ideal and non-ideal cases.

offset position t_ϕ. The sliding window offset in time by the TOF period denotes one period of the responder correlator clock. The time offset period t_ϕ corresponds to the relative phase difference between the initiator and responder illustrated in chapter 4, or $t_\phi = n\Delta t$, where n is the transaction number. Detection positions are illustrated in figure 6.4 for the ideal case (in the absence of noise and accurate Δt) and the non-ideal case (in the presence of noise and inaccurate Δt). As t_ϕ is increased from 0 to E_{dn}, the number of range measurements captured in bin n decreases and the number of range measurements

captured in bin n+1 increases. Phase measurement is extracted by finding the arithmetic mean of the measurements captured in all bins. Considering the three cases and applying the model described by figure 6.4, if device A and B have synchronized correlator clocks, sub-clock phase measurement cannot be obtained because measurement positions only exist at E_{en}, E_{d1}, E_{d++}. If frequency difference exists between A and B, sub-clock phase measurement resolution is bound by Δt ($\Delta t = 1/f_A - 1/f_B$) and n ranging transactions must be performed over the synchronization period to determine the phase measurement. The accuracy of the TOF estimate with phase measurement is bound by the Cramer-rao lower bound for TOF estimates. A set of n ranging samples must be obtained over the synchronization period. If A and B have similar correlator clocks but the relative phase difference is randomly distributed, the corresponding distribution is normal or uniform. For the case of a normal distribution, each range measurement can be considered as a random variable X with a cumulative distribution function over successive measurements assumed to be normally distributed with expectation μ and standard deviation σ. A random sample set of n round-trip measurements $X_1, ..., X_n$ are recorded and the expectation μ is calculated from the sample mean ($\hat{\mu} = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i$). This estimator has error E where $|\hat{\mu} - (t_e + t_l)| < E$ at a particular confidence level. t_e and t_l denote the bounds for early and late range estimates. The size of the sample set $X_1, ..., X_n$ is therefore chosen such that the range estimate is within the error threshold E with an expected confidence within the confidence interval $(t_l - t_e)$. t_e and t_l are calculated from the error of the sample mean of a normally distributed sample by $\bar{\sigma} = \frac{\sigma}{\sqrt{n}}$. The sample number n may then be calculated for a specified ranging error using equation 6.1.

$$E = \bar{X} - \mu = \frac{\mu}{\sqrt{n}} \tag{6.1}$$

$$(t_e + t_l) - E < t_e + t_l < (t_e + t_l) + E \tag{6.2}$$

where μ is the period $t_e + t_l$, σ is the standard deviation, n is the sample size (number of ranging transactions) and $\bar{X}$ is the sample mean. The interval which contains $t_e + t_l$ is given by equation 6.2. The interval in equation 6.2 has fixed end points and the level of confidence is decided by size of the sample set n. The model illustrated in figure 6.4 has been implemented in Python software and the corresponding output characteristic of each aforementioned case has been graphed as shown by figure 6.5. For simplicity, a measured distance of one metre corresponds to one clock period of the transceivers round-trip timer clock. Figure 6.5 illustrates ranging performance for each scenario over two clock periods. In an ideal case where the transceiver clocks are synchronized, $\Delta t = 0$ and the corresponding step-response range estimation function is illustrated by the blue graph line. In the presence of noise, the step-response function becomes skewed and thus

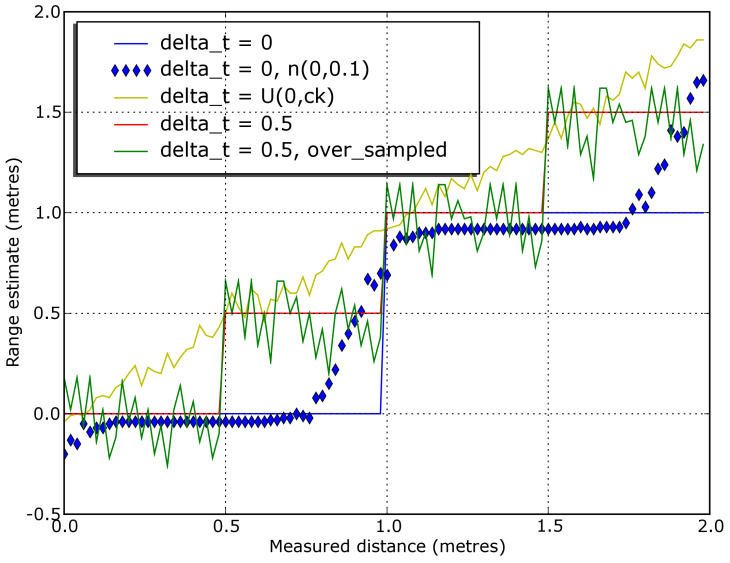


FIGURE 6.5: Effect of error in Δt, over sampling and the ideal condition. $\Delta t = 0.25$ (4 phase measurements per bin period) and t_d is incremented in steps of 0.02 over two bin periods.

the range estimation performance has the characteristic illustrated by $[\Delta t = 0, n(0, 0.1)]$. A normalized noise source is used with 10% effect to illustrate the skew clearly. In order to extract sub-clock phase measurement, a frequency difference Δt must exist. In figure 6.5, Δt corresponds to a measured distance of 0.5 m. In the ideal case where Δt is accurately generated, the corresponding range estimation characteristic is represented by the red line in figure 6.5. Range estimation with sub-clock phase measurement improves range estimation resolution when range measurements are performed multiple times over the synchronization period. However, in the presence of noise, over-sampling over the synchronization period must be performed to reduce the variance in estimates. Over-sampling in the presence of noise produces the green graph line in figure 6.5 and filtering is required to reduce the contribution of this error on range estimates. If the relative phase offset between the initiator and responder is uniformly random, range estimation is linear with increasing distance. The variance of those range estimates is bound by the number of ranging transactions performed. Uniformly random phase offset is challenging to produce and in most instances would rely on noise for its generation. In addition, transceiver clocks typically drift slowly because of the clock synchronization requirements of RF transceivers (i.e. low ppm crystal error). Figure 6.5 shows that range estimation resolution is dependent on the function of the relative phase difference between two devices involved with ranging. If relative phase difference is uniformly random, range resolution is dependent purely on the number of averaged transactions. However, this is at the cost of increasing the time required to determine a range estimate. For this reason and to reduce the complexity of generating uniform offset, it is benificial to use a known frequency difference between the initiator and responder. Similarly, n

packets may be transmitted by the initiator after delay Δt to mimic the relative phase offset between two synchronized devices.

Considering the ranging results and the model presented in figure 6.4, the distribution of the relative phase offset is a complex function and cannot accurately be modelled by a normal or uniform distribution. For this reason, if the responder clock phase offset is a complex function, the resolution of range estimates is said to be bound by the time quantization of the signal correlator and the accuracy of range estimates is dependent on the number of ranging transactions. However, if Δt can be accurately generated and the responder clock remains loosely synchronized, sub-clock range resolution can be obtained. Experimental work relies on the frequency error in crystal oscillators to produce the period Δt. The TI CC2430 crystal oscillator operating at 32 MHz has a frequency accuracy of 80 ppm, this requires that range estimates are performed with significant random delay periods (t>30 ms) in order that the relative phase offset distribution is uniform. Thus, performance improvement can be made either by greater frequency deviation between the initiator and responder or by accurately generated transmission time offset. Figure 6.6 illustrates real-time range estimation for a responder with altered system clock frequency by adding additional load capacitance of 0 pf, 8 pf and 15 pf (nominally used for temperature compensation on the TI CC2430). Range estimation variance is typically less when the responder load capacitance is 0 pf indicating that the transceiver clocks 'drift' to a greater extent. The load capacitance of 15 pf illustrates an almost step-response. The transceiver clocks are closely synchronized in this case and range resolution is bound by the time quantization introduced by the initiator signal correlator. To summarize, the linearity of range estimates may be improved by altering Δt, the frequency difference between the initiator and responder. Using crystal oscillators with known frequency difference would significantly improve the performance of this ranging algorithm. However, using a small frequency difference Δt results in a small non-linear error in range estimation which should be noted. This error can be neglected for two main reasons: 1) its contribution is much smaller than the error resulting from noise; 2) the period Δt must be small in order that the transceivers can synchronize. As illustrated in chapter 4, if the period of the responder clock is less than that of the initiator clock, under sampling occurs and the non-linear characteristic in range estimates increases. Phase measurement cannot be obtained. The period Δt is choosen based on the system application, processing time and require resolution and accuracy.

6.0.2 Noise Performance

The accuracy of range estimates are bound by the receiver's ability to exactly determine the arrival time of a ranging signal. The contribution of noise in the ranging system affects the ability of the receiving device to determine this exact arrival time. In chapter 4 the effect of noise on ranging performance was categorized and illustrated graphically

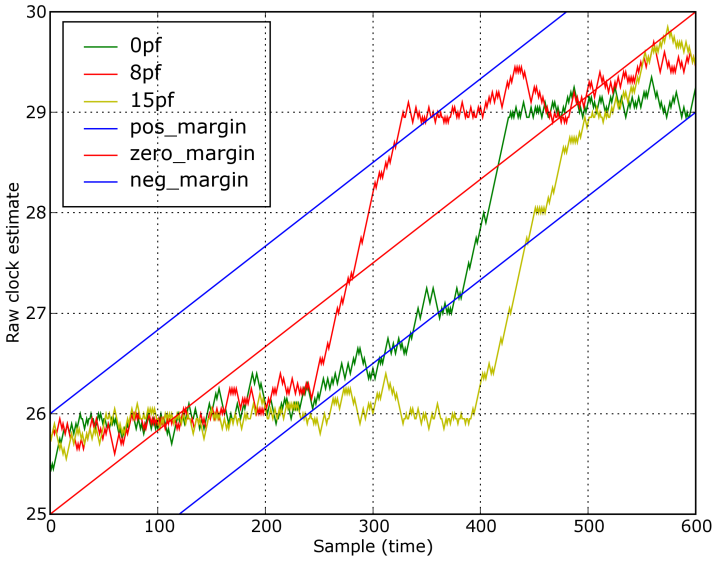


FIGURE 6.6: Two-way ranging performance when changing the load capacitance on crystal oscillator.

using the Cramer-rao lower bound for TOA estimates. Increasing the SNR improves the receivers ability to distinguish the exact signal arrival time. The variance of TOF estimates corresponding to the accuracy is expected to decrease with increased SNR with the relationship illustrated in Figure 3.2. The accuracy should approach the limit given by the CRB for a ranging system with a given signal bandwidth and SNR. Therefore it may be shown that for a two-way ranging system sub-metre ranging accuracy can be achieved using narrow-band 2 MHz signal bandwidth and averaging over multiple ranging transactions. This implies that the narrow-band radio modules used in IEEE 802.15.4 compliant hardware are capable of performing ranging with sub-metre accuracy. To measure this performance experimentally, two TI CC2430 development platforms configured as a transmitter and receiver are placed at a known separation distance. The transmitter continuously transmits and the receiver continually receives. An oscilloscope is used to measure the average signal noise power and average signal power in a shielded environment to prevent the constructive or deconstructive effects of signal multipath. Average noise power is measured at the AFE of the receiver when no ranging signal is transmitted. The process is repeated when a continuous signal transmission is being received at the AFE of the receiving device. SNR is then calculated for different transmission powers enabling ranging variance versus transmit power to be recorded and plotted on a graph using the CRB estimate. Radio transmission power is programmable in 16 steps from -25.6 dBm (current consumption 18.3 mA) to 0.6 dBm (current consumption 32.4 mA) on the TI CC2430 through the TXCTRLL register [55]. It is expected that increased transmission power will improve the systems noise performance and ranging accuracy. The improvement would correspond to the CRB estimate for the calculated SNR and signal bandwidth. However, there are two important points

that should be noted: 1) the CRB indicates that only a linear improvement is gained in the accuracy of TOA estimates by linearly improving the SNR (i.e. using greater signal transmission power). This is not always beneficial because increased transmission power also increases power consumption of the radio and transmission power is regulated by wireless communications standards including IEEE 802.15.4. Furthermore, the SNR has a dynamic range which is both dependent on the initiator - responder separation distance and the properties of the wireless channel. Therefore, TOA ranging parameters can only be calculated for a worst case SNR ratio in the application of the ranging system and this SNR limit should not be exceeded. An SNR of around -20 dB is typically observed and about 85% of communications links have SNR above 10 dB [63]. Applying this average 10 dB SNR value and 2 MHz signal bandwidth to the CRB for two-way ranging denoted by equation 6.3, it is shows that ranging accuracy below 1.0 m is achievable using the IEEE 802.15.4 standard and averaging typically over 100 two-way measurements.

$$\sigma_{TOA} \geq c \cdot \sqrt{\frac{1}{8\pi^2 B^2 \cdot SNR \cdot n}} \geq 0.53m \tag{6.3}$$

This accuracy is better than that predicted by the CRB estimate used in chapter 4 where an SNR of 0.8 was used illustrating the performance of range estimation better than 1.9 m even in a severely noisy environment. The prototype results for the LOS condition over a 250.0 m distance show that the contribution of noise from both the wireless channel and receiver AFE is insignificant in comparison to the timing error introduced from inaccurate clock synchronization or generation of Δt using unsynchronized two-way ranging. At a range of 250.0 m, it is expected that the SNR is much less than at 0.0 m. The variance of range estimates does not change significantly with increasing initiator - responder separation distance illustrated by figure 4.16. Thus, accurately generating the phase measurement period Δt would significantly reduce the variance of range estimates in comparison to increasing the SNR.

6.0.3 Multipath and Shadowing Effects

Multipath and shadowing are a difficult problem for narrow-band communications systems. This is confirmed by our ranging performance results under NLOS conditions where rms error was significantly larger than for the LOS condition (NLOS rms error = 15.8 m, LOS rms error = 7.0 m, 100 averaged samples). In some circumstances, the effects of multipath and shadowing cannot be mitigated and the problem is to minimize their contribution to range estimates. The TI CC2430 employs several algorithms and techniques to reduce the effects of signal multipath and shadowing, however, our NLOS ranging results illustrate that more substantial multipath mitigation techniques are required for ranging. For this reason, different methods are considered to course filter

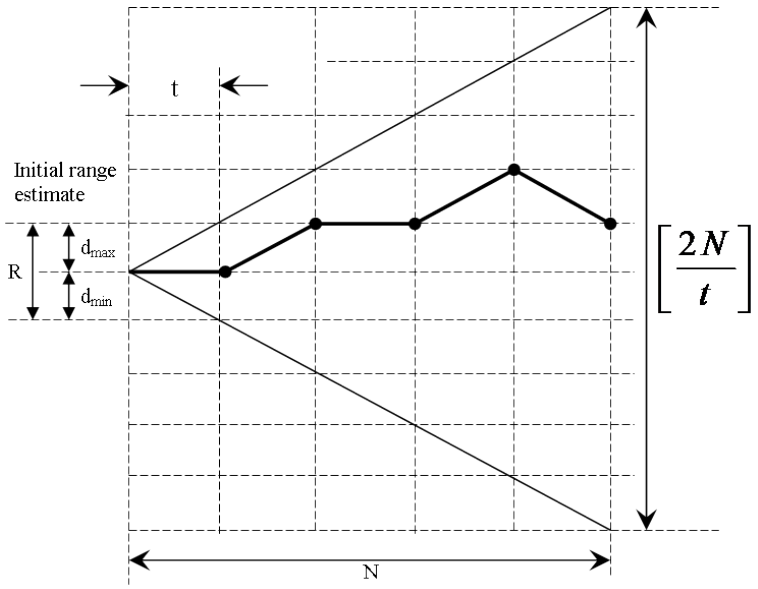


FIGURE 6.7: Filtering technique to reduce multipath, shadowing and noise in range estimates. Real-time continuous range estimates are separated in time by t with maximum rate of change of one filter position (d_{max}/d_{min}) for each of N range estimates.

range estimates over time to reduce the effects of multipath and shadowing, enabling improved range estimate accuracy. The effects of noise contributed by non-random phase offset are also expected between the initiator and responder and inaccurate period Δt are also reduced through course filtering. To meet the constraints of WSNs described in chapter 2, a maximum a posteriori (MAP) estimation technique used for the frequency synchronization of multiple frequency shift keying (MFSK) during demodulation is used to filter range estimates [82]. Alternative filtering techniques could also be implemented but their cost would require evaluation for the filtering of range estimates in WSNs. The simplicity of this filtering technique makes it particularly suitable for ranging in WSNs under the constraints of resource constrained hardware. The filter is described graphically in figure 6.7. Parameter t is the separation time between range estimates, N is the total number or continuous number of estimates, d_{min} and d_{max} are the maximum and minimum step change of range distance estimation between range estimates and R is the estimation window. Over a sample set of N range estimates, the maximum change in range estimate distance is $[2N/t]$. Filter parameters including t and R are preset by the ranging system. The maximum and minimum change in range estimate distance is then chosen to meet the requirements of the ranging application. For example, if the ranging application is real-time tracking, the fastest moving object may be 2 ms^{-1} (person walking), d_{max} and d_{min} must therefore allow for a range estimate change of ± 2 ms^{-1}. If the separation time between range estimates is 0.25 s, d_min and d_{max} must correspond to a range estimate distance of 0.5 m. Figure 6.8 illustrates the performance of the ranging algorithm with the aforementioned filter technique implemented in Python software. The initiator and responder are placed together and then moved apart in 2.0 m increments over a distance of 16.0 m for LOS conditions. Figure

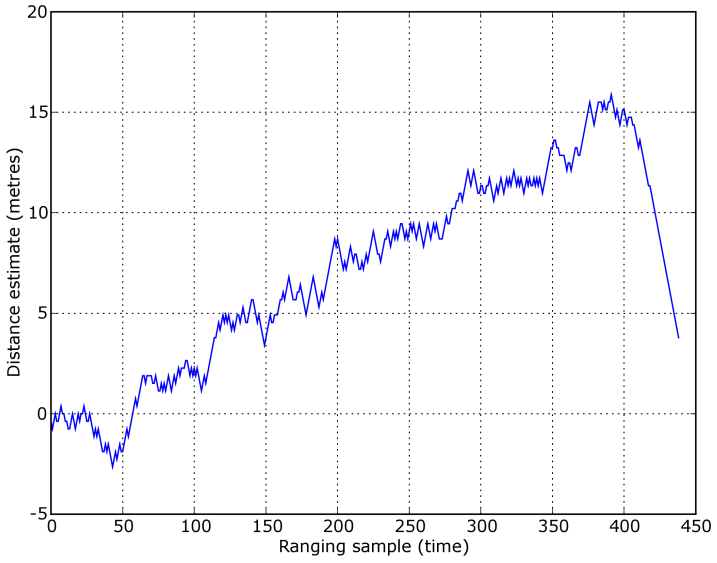


FIGURE 6.8: Real-time performance of ranging algorithm with filter implementation.

6.8 shows that the accuracy of range estimation is significantly improved using course filtering because the variance in range estimation is typically much less than found for the prototype raw results illustrated in chapter 4. However, experimentation work has shown that the level of filtering required limits the real-time distance estimation capability of the ranging system. Figure 6.8 also shows more closely the effect of SNR on ranging performance. At short range initiator-responder distance (<5.0 m), the SNR is large and the receiver has good ability to distinguish the exact TOA of the ranging signal. At longer seperation distance (>5.0 m), the SNR is smaller and the exact TOA of the ranging signal cannot be as easily distinguished. The effect of SNR is illustrated by the decreasing incremental range estimate steps in figure 6.8.

Chapter 7

Conclusions

Wireless sensor networks consisting of inexpensive resource constrained sensor devices hold promise for many monitoring, control and tracking applications. Knowledge of the position of those sensors is a fundamental requirement to make use of data recorded by individual sensing nodes within those wireless networks. Position information can be recorded during deployment of sensors, however, in some circumstances this is not a valid approach and a localization mechanism is required. The focus of this research has been to estimate the point-to-point distance between two sensor nodes involved with the localization process of a WSN. A novel RF TOF ranging system has been developed and its performance for localization has been demonstrated through the development of a basic locating system. The following conclusions have been drawn for the research herein.

7.1 Summary of Work

Radio frequency ranging for wireless sensor networks

A novel narrow-band two-way TOF ranging method with phase offset measurement has been successfully implemented and demonstrated using low frequency clocks to determine range measurements with accuracies better than 7.0 m LOS, 15.8 m NLOS and 1.7 m indoor using hardware suitable for WSN applications. The ranging algorithm operates time dependently using the principle method of the Vernier delay line. This technique is not frequency dependent in comparison to alternative TOA based ranging algorithms. The developed algorithm operates on a single-chip solution without the requirement of additional hardware overheads. To the best of the authors' knowledge, this is the first time-dependent RF TOF ranging scheme to exploit the relative offset in frequency between two radio transceivers involved with TOF ranging in order to improve ranging resolution. The technique therefore has substantial benefits in WSNs where sensor

nodes are required to operate with low power consumption and thus a low system clock frequency. In addition, the use of conventional narrow-band RF enables the operation of this ranging system within regulation over greater range (>50 m) than alternative UWB based ranging systems. The algorithm is compatable with IEEE 802.15.4 but could similarly be implemented in other subsequent standards such as IEEE 802.11.

The resolution of the prototype system is limited by the frequency difference Δt and the accuracy is bound by three fundamental factors including: (1) the variance in time delays of the transceiver analogue front end and processing delays; (2) the accuracy of the generated period Δt; (3) the signal-to-noise-ratio (SNR). The time taken to achieve a specified degree of accuracy is limited by the bandwidth of the signal correlator. It is expected that the recorded variances in our results are greater than expected because of the error contribution caused by referencing range estimates to GPS. Furthermore, error in the minimum round-trip calibration also contributes a small error.

One previous RF TOF ranging system (frequency dependent) prototyped by T. C. Karalar and J. Rabaey [17] reports an RF TOF ranging scheme with estimation accuracy within -0.5 m to 2.0 m using an FPGA with 100 Msps ADC sample rate. Ranging accuracy in this scheme is improved by increasing the sample rates of the signal ADC and DAC. In this work a TI CC2430 has been used with determined signal sampling of 8 Msps and a TOF phase offset scheme to achieve ranging accuracy below 7.0 m RMS under LOS conditions using 100 averaged samples. Ranging accuracy is improved by increasing the number of ranging transactions. This is more suitable for WSN applications where sensor nodes operate from low-frequency system clocks to maintain the life of the sensor network. The performance of this ranging technique may be improved by using a known frequency difference between the transceivers in order to obtain an expected Δt. This enables the required ranging resolution to be obtained within an expected time period. Furthermore, the arbitrary chosen sample number N can be replaced by considering the variance in the round-trip time measurement distribution to automatically perform the required number of ranging transactions N for a specified ranging accuracy.

Localization for wireless sensor networks

A prototype RF TOF based locating system has been demonstrated which is suitable for the localization process of WSNs or as a LPS. Evaluation and testing has been carried out using a standard TI CC2431 development kit. To the best of the author's knowledge, this is the first RF-based locating system to operate using low frequency clocks and no wired connectivity between references for data transfer and synchronization. Resolution and accuracy is bound by the performance of the ranging systems ability to correctly estimate the point-to-point distance between a blind device and a set of known references. Position estimates are determined using a grid-search and simplified optimization method with a resolution of 0.2 m in order to meet the requirements of WSNs and enable real-time position estimation (latency $<$ 2 s). This approach is

computationally intensive without the addition of an optimizer to reduce the number of position computational estimates. Resolution of this algorithm may be improved at a cost of increased processing time of a position estimate, thus limiting the systems ability to compute position estimates real-time. Alternative UWB locating systems have demonstrated excellent performance (precise resolution and accuracy) both indoors and outdoors using bandwidths greater than 500MHz. In comparison, the locating system herein operates using narrow-band (2 MHz) signals and a low-frequency (8MHz) signal correlation clock to enable position estimation accuracy better than ± 1.0 m for over 75% of position estimates under LOS conditions and an accuracy of better than ± 1.5 m for over 55% of position estimates for NLOS conditions. The locating system herein enables real-time position estimation of a blind sensor node within the accuracy and an resolution requirements of WSNs (resolution better than 0.3 m, accuracy better than ± 1.0 m for 50% of estimates LOS, accuracy better than ± 2.5 m for 50% of estimates NLOS). In comparison to alternative UWB-based locating systems, this system enables position estimation within regulation over greater distance (> 100 m) and the ability of ranging to be performed within widely used narrow-band radio systems. As a comparison, the PAL650 UWB-based locating system by multi-spectral solutions can determine 7883 position estimates in 2.2 hours [21]. The prototype RF-based locating system herein computes a single position estimate in less than two seconds. It is expected that the prototype locating system could be further developed to enable three-dimensional position estimation and real-time tracking of assets in both LOS and NLOS conditions with significantly larger numbers of blind devices.

7.2 Suggested Further Work

Radio Frequency Time-of-Flight Ranging

In chapter 4 the relative phase offset ϕ_p between the initiator and responder over successive two-way TOA measurements was assumed to be random and normally distributed. This assumption was made on the basis that the initiator and responder clock periods are sufficiently inaccurate and inherit significant noise from the system. Our results analysis in chapter 6 concluded that this was simply not the case and the phase offset distribution over successive two-way TOA measurements is a complex function which changes with initiator-responder distance. For those reasons, it has been concluded that the initiator and responder clock periods used to generate the frequency difference Δt must be more accurately generated in order to deduce the required number of two-way transactions and obtain the phase offset measurement to higher accuracy. The initiator and responder may be clocked from independent signal generators to confirm this result, where the complex function of the relative phase offset over successive two-way transactions is removed and Δt can be accurately determined. The resolution and accuracy of the system can then be decided by the developer in order for the system to meet the

requirements of the application. A further averaging over this synchronization period can then be used to reduce the variance in the estimates through the contribution of noise.

In chapter 4 the TI CC2420s relative phase drift was illustarated using an initiator and responder and digital storage oscilloscope to capture the drift period. This result concluded that the TI CC2420 receiver could successfully perform signal lock within a single clock period of the signal correlators clock assuming a correlation frequency of 8 MHz. Further research is necessary to investigate the ADC value at the instance of signal lock. Correction for the phase offset time is required to reduce range error since the ADC correlation value will remain consistent for each two-way measurement. A solution is to average the values over successive ADC values to reduce the effects of noise. In the current system, no algorithm is employed to correct for the phase offset in the ADCs correlation value as it has been assumed that the relative phase offset between the transceivers is random and that the offset in this case would not affect the performance of this system. Using known frequency difference it is expected that the phase offset correction would enhance the performance of the algorithm. The effects of noise could be reduced by averaging the corelation value over multiple correlations during receiving the preamble sequence and SFD byte of ranging packets.

In addition to the aforementioned improvements, it is expect that the following implemented algorithm would also significantly improve the performance of the ranging algorithm. It has been demonstrated that with the use of a simple filter the contribution of noise on round-trip measurements can be significantly reduced. The choice of filter was based on simplicity and the application of the system would fundamentally decide the appropriate choice of filter method. However, wireless sensor nodes are resource constrained, low complexity and must also operate with low power consumption, hence this filter method is sufficient and demonstrates acceptable performance. However, implementation of a different filter may improve the performance of range estimation for real-time tracking. It is also expected that a significant noise contribution is generated in the front end of the receiver. It is expected from the drift period obtained from test that noise variance of up to 15 ns is added by the front end, however, a significant amount of noise can be reduced through filtering.

RF Time-of-Flight based Local Positioning System (LPS)

The position estimates of blind sensor nodes are significantly affected by the ability to accurately determine point-to-point range between the blind device in question and a set of fixed references. Therefore, the contribution of noise and signal multipath to range estimates must be reduced to enhance the performance of the locating system in question. Position estimation in two-dimensions is executed using a brute-force method that requires additional algorithms to account for multipath propagation error. The algorithm is computationally intensive due to the number of position estimates calculated

for each individual position estimate. Therefore, the position computational process requires further development to reduce the processing overheads by using a course grid search followed by either Kalman filtering, particle filter or optimization methods. Previous research has demonstrated that optimization techniques have clear advantages when processing capabilities are restricted because of their simplicity in comparison to alternative position computational methods. Position estimation requires development to enable its adaption for real-time tracking of assets and personnel in both LOS and NLOS conditions with significantly larger numbers of blind devices. Extension of the methods to enable position estimation in three-dimensions is also a requirement for locating in multi-story buildings.

Appendix A

Publications

- B Thorbjornsen and N M White and A D Brown and J S Reeve, Radio frequency (RF) time-of-flight ranging for wireless sensor networks, Measurement Science and Technology, vol. 21, no. 3, pages 035202, 2010.

IOP PUBLISHING MEASUREMENT SCIENCE AND TECHNOLOGY
Meas. Sci. Technol. **21** (2010) 035202 (12pp) doi:10.1088/0957-0233/21/3/035202

Radio frequency (RF) time-of-flight ranging for wireless sensor networks

B Thorbjornsen, N M White, A D Brown and J S Reeve

Electronics and Computer Science, The University of Southampton, Southampton SO17 1BJ, UK

E-mail: bt05r@ecs.soton.ac.uk

Received 3 June 2009, in final form 26 October 2009
Published 25 January 2010
Online at stacks.iop.org/MST/21/035202

Abstract
Position information of nodes within wireless sensor networks (WSNs) is often a requirement in order to make use of the data recorded by the sensors themselves. On deployment the nodes normally have no prior knowledge of their position and thus a locationing mechanism is required to determine their positions. In this paper, we describe a method to determine the point-to-point range between sensor nodes as part of the locationing process. A two-way time-of-flight (TOF) ranging scheme is presented using narrow-band RF. The frequency difference between the transceivers involved with the point-to-point measurement is used to obtain a sub-clock TOF phase offset measurement in order to achieve high resolution TOF measurements. The ranging algorithm has been developed and prototyped on a TI CC2430 development kit with no additional hardware being required. Performance results have been obtained for the line-of-sight (LOS), non-line-of-sight (NLOS) and indoor conditions. Accuracy is typically better than 7.0 m RMS for the LOS condition over 250.0 m and 15.8 m RMS for the NLOS condition over 120.0 m using a 100 sample average. Indoor accuracy is measured to 1.7 m RMS using a 1000 sample average over 8.0 m. Ranging error is linear and does not increase with the increased transmitter–receiver distance. Our TOA ranging scheme demonstrates a novel system where resolution and accuracy are time dependent in comparison with alternative frequency-dependent methods using narrow-band RF.

Keywords: wireless sensor network (WSN), locationing, ranging, time-of-flight, two-way, phase measurement, narrow-band, synchronization, algorithm, integrated

(Some figures in this article are in colour only in the electronic version)

1. Introduction

The development of fully integrated, low-power, low-cost communications equipment over recent years have led to the development of wireless sensor networks (WSNs) for many monitoring, control and tracking applications [1–3]. Determining the position of sensor nodes within those networks is important in order to provide additional information to the quantity being measured. Sensor nodes are often deployed without a prior knowledge of their location and therefore a method to determine their absolute or relative position is required.

To locate 'blind' sensor nodes, a ranging or angle measurement is first made to a number of reference or 'anchor' nodes which have prior knowledge of their location with respect to a local or global coordinate system. An algorithm is then used to compute the position of the blind device in relation to the reference nodes. Thus, the process of locationing consists of two stages: (1) ranging or angle measurements; (2) the computation of the position of the blind device. In this paper, we focus on the problem of accurately estimating the point-to-point distance between two sensor nodes involved with the localization process of a WSN. Computation of a blind device position will be considered in our following publication.

There are five main methods of determining point-to-point distance. These include time-of-arrival (TOA) [4, 5], time-difference-of-arrival (TDOA) [3, 6], received-signal-strength-indication (RSSI) [7], near-field-electromagnetic-ranging (NFER) [8] and angle-of-arrival (AOA) [9]. Ranging in WSNs is challenging because of the constraints of sensor

 © 2010 IOP Publishing Ltd Printed in the UK

nodes and the accuracy requirements of the locationing mechanism. Ranging accuracy is typically required below 1 m using simple hardware and resource-constrained sensor nodes with low-power operation (<27 mA transmit, 25 mA receive using 2–3.6 V supply in active mode [10]). Those sensor nodes also operate in an unsynchronized manner from inaccurate crystal device clocks ($C_0 \pm 40$ ppm without temperature compensation [10]). In addition to the technical challenges, low cost and physical size limitations also set stiff constraints. TOA and RSSI are the most widely used ranging methods.

TOA ranging involves the measurement of the transit time of a signal in order to estimate point-to-point distance. Its ability to operate well in high multipath environments and provide sub-metre ranging accuracy has been demonstrated using ultra-wideband (UWB) [6].

In contrast, RSSI involves measuring the attenuation of a signal through the wireless channel to estimate the transmitter–receiver distance. The simplicity of this technique has led to its implementation on many WSN hardware platforms. The requirement for complex models that are able to remove the large errors caused by signal multipath can limit the accuracy of RSSI.

NFER involves the measurement of the phase change of a signals magnetic and electric component to estimate distance. NFER operates on very low frequencies (within the AM broadcast band 530–1710 kHz) hence benefiting exhibiting propagation properties. However, as with UWB-based TOA ranging, this technique can interfere with other systems, and therefore, the Federal Communications Commission (FCC) limit the maximum transmission power. For this reason, UWB-based TOA and NFER ranging methods can only operate over a short range (<60 m) [8].

TDOA uses a set of synchronized reference nodes at known locations to determine the TDOA of ranging signals to or from a blind node for localization. Wired infrastructure is a requirement between the references to meet the timing requirements and transfer data. This is a costly overhead and limits TDOA applications to fixed referencing architectures.

AOA involves the use of complex antenna arrays to measure the arrival angle of a received signal. The requirement of complex antenna arrays make AOA an impractical solution for sensor nodes due the physical size of those antennas [4].

In this paper, we consider a narrow-band RF TOF ranging approach to meet the constraints posed by WSNs and accurately estimate the point-to-point range. Alternative TOF ranging schemes have used UWB signals to achieve sub-metre ranging resolution [6]; however, those are limited in the operational range (<100 m) because of the FCC regulation on transmission power. To meet the sub-metre ranging resolution using narrow-band RF, we consider the frequency difference between the transmitting and receiving device in order to measure sub-clock phase offset of received TOA signals. This approach is time dependent in comparison to alternative frequency-dependent techniques [4].

The algorithm, in its prototype, has been designed and tested using a TI CC2430 development kit. Ranging transactions are carried out using the 2.4 GHz ISM band on a single channel with the algorithm being developed for its compatibility with the IEEE 802.15.4 standard. The algorithm can similarly be implemented in other comparable communication schemes incorporating different modulation techniques.

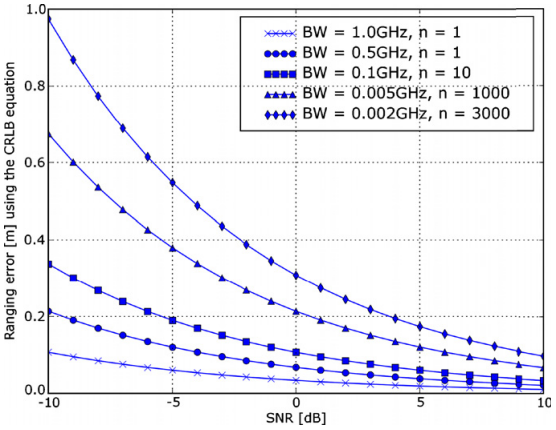


Figure 1. Lower bound of time-of-arrival ranging errors.

The remainder of this paper is organized as follows: section 2 details the preliminaries involved with TOA ranging; section 3 describes the ranging system; section 4 details the implementation of the prototype system and the expected accuracy; section 5 shows the preliminary testing results for the prototype system for LOS, NLOS and indoor conditions; and section 6 summarizes and concludes the research.

2. Preliminaries

2.1. Cramer–Rao lower bound for time-of-flight ranging estimates

The Cramer–Rao is an unbiased estimator for the lower bound variance of TOF measurements defined by equation (1) [11]. The variance (TOF time error) is defined as σ^2_{TOF}, β_f (Hz) is the spectral bandwidth of the received signal, n is the number of averaged TOF measurements and SNR is the energy per bit divided by the noise power (E_b/N_0):

$$\sigma^2_{\mathrm{TOF}} \geqslant \frac{1}{8\pi^2 \cdot \beta_f^2 \cdot \mathrm{SNR} \cdot n}. \tag{1}$$

From (1) it can be seen that a quadratic improvement to TOF estimates is made through increasing the signal spectral bandwidth, and hence is the reason why UWB is a good approach for accurate TOF ranging. Furthermore, the SNR is linearly proportional to TOF variance. The Cramer–Rao lower bound range distance error is defined as the product $c \cdot \sigma_{\mathrm{TOF}}$, where c is the speed of light [12]. Figure 1 shows Cramer–Rao lower bounds on the ranging error for five different spectral signal bandwidths with n averaged samples. It can be seen that sub-metre ranging accuracy can be achieved by using a spectral bandwidth of as low as 2 MHz and averaging 3000 samples ($n = 3000$). In contrast, if the signal spectral bandwidth can

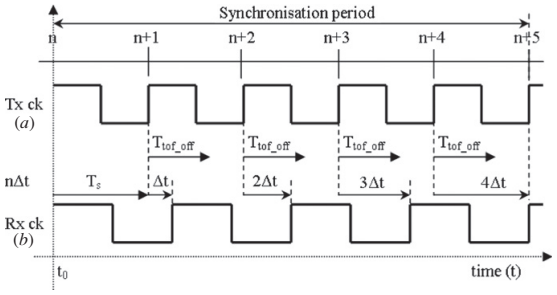


Figure 2. Schematic view of TOA phase measurement using correlator frequencies T_s and $(T_s + \Delta t)$ over successive range measurements. Transmit and receive assumed on rising clock edges.

be increased, a quadratic gain is made. This is not always ideal because of the FCC regulation on transmission power using ultra-wideband. Using less bandwidth and averaging greater numbers of ranging measurements is therefore a favourable approach. Time averaging has also been found to reduce the effects of multipath signal propagation and additive white Gaussian noise (AWGN) [12]; however, the use of multiple measurements increases the processing time which may introduce limitations on the estimation time and hence limit the applications of the ranging scheme (i.e. make it unsuitable for real-time tracking systems). For those reasons, a trade-off must be made in the choices of system parameters including signal bandwidth, signal power, chip-rate and ranging accuracy requirement.

2.2. Measurement resolution

In alternative narrow-band RF TOF measurement systems, resolution is limited by the time quantization introduced by the sampling period of the receiver's signal correlator [4], we denote this by equation (2). ΔR is the TOF ranging resolution (m), c is the speed of light (m s^{-1}) and T_s (s) is the sampling period of the receiver signal correlator:

$$\pm\Delta R = \frac{cT_s}{2}. \tag{2}$$

Ranging resolution in WSN applications is typically required to be within ± 1 m, and therefore $T_s \leqslant 6.66$ ns; this corresponds to a signal correlator sampling rate $F_s \geqslant 150$ MHz [4]. This is not ideal in low-power WSN hardware because of the increased power requirements of higher frequency oscillators ($I[\mathrm{A}] = \mathrm{d}Q/\mathrm{d}t$, as $\mathrm{d}t \to 0$, $I \to \infty$). For this reason, we consider a novel time-dependent TOF ranging method as an alternative to frequency-dependent methods. We achieve $T_s \leqslant 6.66$ ns by considering ranging transactions between a transmitter and receiver with signal sampling periods T_s and $(T_s + \Delta t)$. The time difference Δt allows sub-clock phase offset measurement over multiple ranging transactions as shown in figure 2. Ranging transactions arriving at the receiver before $T_{\mathrm{tof\_off}}$ have period τ and are binned in b_0. Ranging transactions arriving after $T_{\mathrm{tof\_off}}$ have $\tau + 1$ clock periods and are binned in b_1. $T_{\mathrm{tof\_off}}$ corresponds to the sub-clock period or phase measurement of the TOF period. The number of ranging transactions n required to obtain the phase offset measurement is determined from $n = T_s/\Delta t$, and we define this as the synchronization period. The TOA period with phase offset measurement is finally extracted by finding the arithmetic mean as shown in equation (3):

$$\tau_{\mathrm{TOF}} = \frac{1}{n}\sum_{i=1}^{n}(b_0 + b_1). \tag{3}$$

Ranging transactions are offset by one clock period for each measurement with the constraints $(0 < \Delta t \leqslant 0.5T_s)$ and Δt divisible by T_s in order to achieve TOA ranging with phase offset measurement. The period Δt fundamentally limits the resolution of the TOF estimates. The effects of noise, multipath signal propagation and frequency inaccuracies may be reduced by oversampling over the synchronization period. Using this technique, TOF ranging estimates are time dependent as opposed to the previous frequency-dependent methods. The phase measurement principle can be seen from the Vernier delay line [13], where in this implementation, the function of the two buffer delay lines is generated through the frequency difference Δt. The transmission time and period of the transmitter clocks are required at the receiver in order to recover the TOF period; this is achieved through synchronization detailed in the next section.

2.3. Synchronization

There are two constraints relevant to the evaluation of TOF measurements: (1) the transmitting (Tx) and receiving (Rx) devices must be precisely synchronized to a common system clock (ck) and (2) the receiving device must be provided with the transmission time of the ranging signal. From this perspective, a signal is transmitted from some device A at a known time $(t_{A\text{-transmit}})$ and is detected at a measured time $(t_{A\to B})$ with reference to a common system time. There are two methods of synchronizing the devices A and B categorized as one-way transaction and two-way-time transfer (TWTT).

2.3.1. One-way ranging. With a one-way ranging transaction, synchronization between the transmitter and receiver devices is achieved by the use of different signal frequencies. An electromagnetic signal is used to synchronize the devices and a slower acoustic signal is used to measure the TOF [14].

2.3.2. Two-way time transfer. The two-way-time-transfer technique [15] is illustrated in figure 3 where devices A and B incorporate transceivers as opposed to a single transmitter and receiver. The method is used to compare two clocks or oscillators in order to reduce the phase offset (in clock cycles) and hence synchronize the devices. A and B operate from independent system times which are unsynchronized and have some phase offset where the resolution of the technique is bound by the period of the clock at device A. The phase offset and signal TOF between A and B are derived from equations (4)–(7), where $(t_{A\text{-transmit}})$ and $(t_{B\text{-transmit}})$ are the transmit times, $(t_{A\to B})$ and $(t_{B\to A})$ are the received times, (t_{tof}) is the time-of-flight period and $(t_{B\text{-offset}})$ is the phase offset

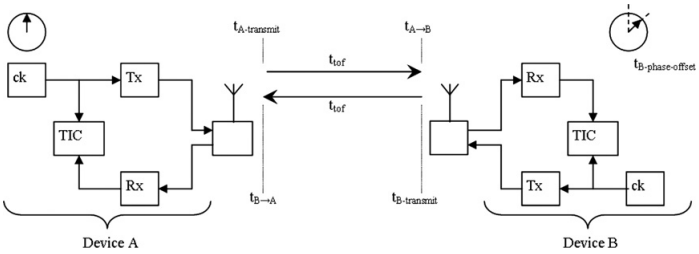


Figure 3. Two-way time transfer method for synchronization [15].

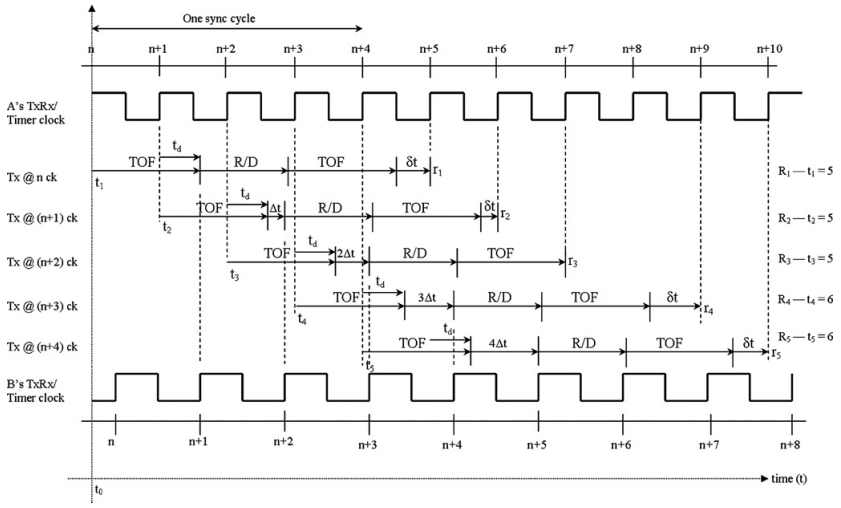


Figure 4. Timing diagram of two-way time-of-flight ranging with phase measurement.

of device B's clock with respect to device A's clock. The unsynchronized two-way time transfer measurements include the phase offset as an additive term in the forward transfer and a subtractive term in the reverse transfer with respect to A's clock. The additive phase offset can be removed by averaging multiple two-way transfers and hence an accurate TOF period is obtained. The TOF period is extracted from the time interval counter (TIC) or free-running timer. This is then calibrated to correspond to the true distance d[AB] by using $d[\mathrm{m}] = \tau c$, where c is the speed of light (3×10^8 m s^{-1}):

$$t_{A\to B} = t_{A\text{-transmit}} + t_{\mathrm{TOF}} + t_{B\text{-offset}}, \quad (4)$$

$$t_{B\to A} = t_{B\text{-transmit}} + t_{\mathrm{TOF}} - t_{B\text{-offset}}, \quad (5)$$

$$t_{\mathrm{TOF}} = \tfrac{1}{2}[(t_{A\to B} + t_{B\to A}) - (t_{A\text{-transmit}} + t_{B\text{-transmit}})], \quad (6)$$

$$t_{\mathrm{offset}} = \tfrac{1}{2}[(t_{A\to B} - t_{B\to A}) - (t_{A\text{-transmit}} - t_{B\text{-transmit}})]. \quad (7)$$

3. Ranging system

To satisfy the synchronization requirement between two devices involved with TOF ranging, we use two-way ranging transaction in order to perform unsynchronized TOF measurements as illustrated from a time perspective in figure 4. Devices A and B operate from clocks with known periods t_1, t_2 where Δt is the difference in the period. We define the synchronization period as the number of cycles of clock A for which A and B are out of phase as shown in figure 2. Two-way ranging transactions are exchanged between the devices for each incremented period of clock A to obtain sub-clock period phase measurements over the synchronization period. The scheme operates by devices A and B first committing to perform TOF ranging and agreeing a common channel. Following this stage, two-way ranging transactions are made between A and B. Device A transmits a ranging message to device B. During transmission, A reads and stores the value of a free-running timer. After a TOF propagation period corresponding to the distance AB, the message arrives at B, which receives this message on its next clock edge after $n\Delta t$, where n is the phase measurement number. After a fixed period response delay (R/D), B transmits a ranging transaction back to A. Following the return TOF period, A receives the ranging message after a period δt and again stores the value of the free-running timer. The two-way period is determined by subtracting the final stored value from the initial stored value. This process is repeated with each two-way measurement shifted in time by one clock period over the synchronization cycle to obtain the round-trip estimates including a phase offset term. The period δt does

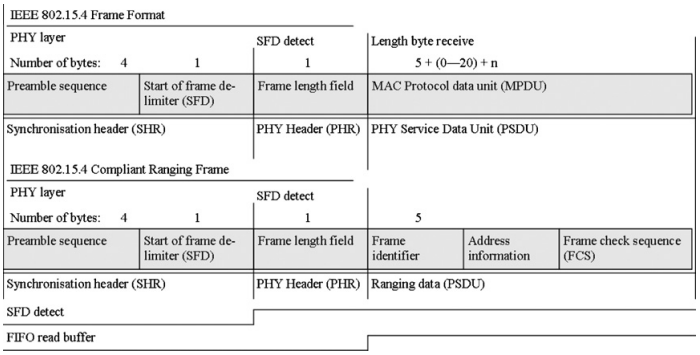


Figure 5. Schematic illustration of the IEEE 802.15.4 compliant ranging frame.

not affect phase measurements since its period is always less than one cycle of A's clock. Phase measurement resolution Δt is decided by the frequency difference between A and B where Δt is incremented for each measurement by transmitting on the next successive clock edge.

The TOF period with phase offset measurement t_d is then computed by equation (3) for n measurements over the synchronization period. This estimate is then converted to a distance estimate by executing three steps: (1) obtaining the calibrated round-trip period by subtracting the minimum round-trip period (when the distance A–B is zero) from the mean estimate round-trip period; (2) obtaining a single TOF period by dividing the calibrated estimate round-trip period by 2; (3) using the relationship $\Delta s = v\Delta t$ to convert from time to distance.

4. System implementation

4.1. Prototyping platform

A Texas Instruments TI CC2430 development kit [16] was selected to prototype the two-way TOF ranging system. The TI CC2430 is a fully integrated 2.4 GHz RF transceiver and Intel 8051 MCU particularly suited for personal area network (PAN) applications compliant with the Zigbee and IEEE 802.15.4 protocol. The RF radio module operates with direct sequence spread spectrum (DSSS) modulation with a 2 Mb s^{-1} chip-rate to produce a 250 kb s^{-1} data rate in the 2.4 GHz ISM frequency band [17]. To extract round-trip timing for TOF measurements, we use the TI CC2430s high-frequency 32 MHz crystal oscillator and medium access control (MAC) capture timer.

4.2. Frame format and timing extraction

The TI CC2430 supports the IEEE 802.15.4 frame format described fully in [17] consisting of a synchronization header (SHR), physical (PHY) header and PHY service data unit (PSDU). Its compliant adaption for TOF ranging is shown in figure 5 as transmitted by the PHY layer from left to right.

The synchronization header consists of a preamble sequence followed by a start-of-frame delimiter (SFD). During receive mode, the synchronization header is used by the transceiver signal demodulator to identify and synchronize to the incoming data frame. On reception, the transceiver frequency adjusts and synchronizes to the received preamble sequence. Compliant packets are identified by a continuous search and correlating the received preamble sequence with a local copy. The physical header also known as the frame length field defines the number of bytes in the MAC protocol data unit (MPDU) or PSDU. This field is implemented to make data frames compliant with IEEE 802.15.4 but is not essential for TOA ranging packets. To make the IEEE 802.15.4 frame efficient and suitable for TOF ranging measurements, only the synchronization header, PHY header and a PSDU consisting of an identifier, address information and check sequence are used. This corresponds to ranging packets which are 11 bytes in length.

Timing extraction for TOF estimation is provided through the SFD byte. On reception and synchronization of compliant packets, the SFD byte triggers timing extraction via a free-running timer. The TI CC2430 incorporates a 16-bit MAC timer which is configurable to capture the rising edge of the SFD on transmission and reception of ranging frames. This is configured to free-run and the round-trip period is extracted by subtracting the final timer value from the initial timer value. Switching between transmit and receive mode of the transceiver is performed through software for each two-way measurement.

4.3. Time-of-arrival estimation algorithm

Two-way TOF ranging is performed between two TI CC2430 development platforms which are flash programmed independently as an 'initiator' and 'responder'. For the purpose of testing, the address of the responder and the number of ranging transactions to be executed are pre-programmed on to the initiator prior to the ranging process. A ranging packet identifier is also predefined as a single byte. High level software flow diagrams for the initiator and responder are shown in figures 6 and 7.

To initiate the ranging process, the initiator device A requests to perform ranging with the responder device B by transmitting a 'request to range' (RTR) packet. Assuming

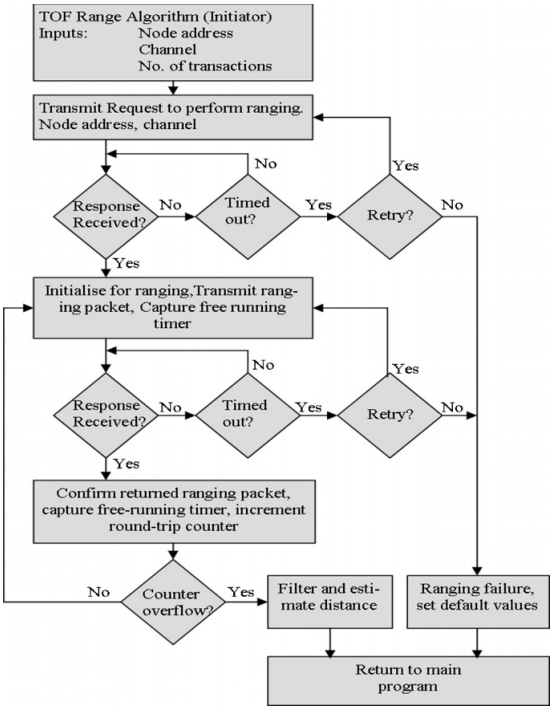


Figure 6. High level ranging algorithm flow diagram for an 'initiator' device.

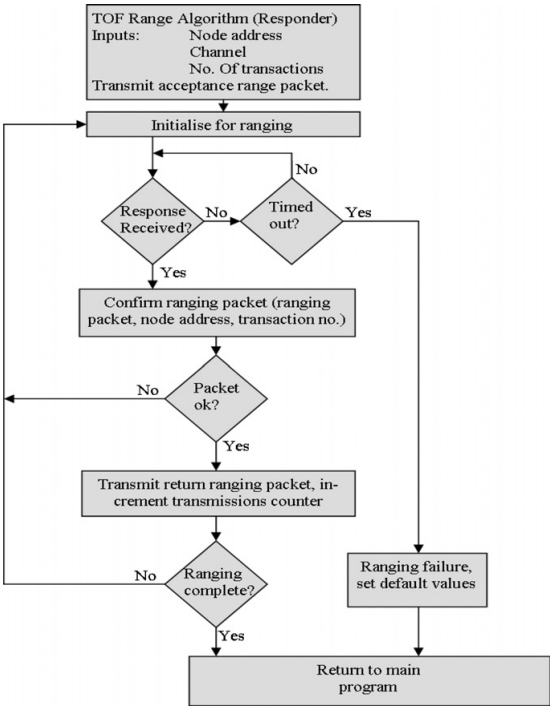


Figure 7. High level ranging algorithm flow diagram for a 'responder' device.

that device B is within a radio range of A and the packet is not lost, B receives and acknowledges the 'request to range' message by transmitting an 'acceptance to range' (ATR) packet back to A. Assuming arrival of the ATR packet at A within an appropriate time period, A initializes itself to perform ranging. The RF radio is configured and the agreed channel for ranging is selected. The round-trip timer is configured to operate as a free-running capture timer with capture activated by the rising edge of the SFD detect. A ranging packet is then transmitted to B with the value of the free-running timer captured on transmission. Device A switches to receive mode and waits for a return ranging packet from B. If the return ranging packet is not received within a time-out period, the ranging transaction is presumed 'lost' and the ranging packet is re-transmitted. Three re-transmission attempts are made before the ranging process is regarded as a 'failure'.

On reception of a packet at device A following previous transmission of a ranging packet, the packet preamble sequence and SFD trigger the capture of the free-running capture timer. Device A checks the identity of the packet and if as expected (i.e. a ranging packet), the round-trip measurement is calculated by subtracting the transmit time from the receive time. This value is stored and the ranging transaction counter is incremented to indicate the number of successfully completed ranging transactions. If a corrupted or incorrect packet is received, the round-trip measurement is disregarded. The process is repeated until the required number of ranging transactions have been achieved. The distance estimate with phase offset measurement is then computed and filtered as required. Ranging is complete and the estimated distance is returned to the main program.

From the perspective of the responder B, a 'request to range' (RTR) packet is received from device A. This packet contains the address of device A which is requesting to range with B, the channel on which ranging should be executed and the number of ranging transactions to be performed. Assuming that device B has the corresponding packet address, the ranging process can be executed. B acknowledges the RTR by transmitting an 'acceptance to range' (ATR) packet back to A and then enters a waiting loop ready for a ranging packet to be received from device A. If no ranging messages are received within the waiting loop, the loop times-out and the ranging process is regarded as a failure. The radio module and round-trip timer are returned to their default values before the ranging algorithm is exited. The main program receives a set of standard values in the case of a ranging failure. Alternatively, when a packet is received, B confirms the packet type, checks its validity and stores the transaction number. If the parameters are as expected, B transmits a return ranging packet back to A. This process is always executed over the same number of system clock cycles in order that the phase offset can be obtained. Alternatively, if the received packet is corrupt or of an incorrect type or format, B returns to its waiting loop ready to receive the next ranging packet. Following completion of all ranging transactions, B returns all hardware device values to their defaults and jumps back to the main program.

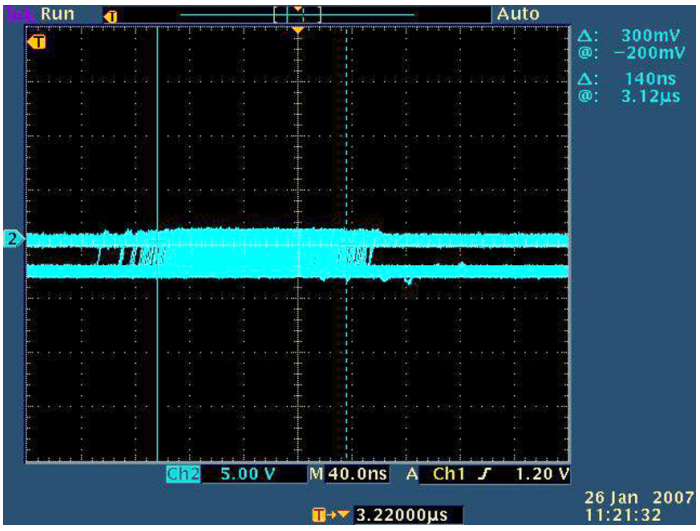


Figure 8. Digital storage oscilloscope capture of the TI CC2420 correlator drift over the 140 ns period.

4.4. Interference issues

The two-way TOA ranging system is prototyped using the TI CC2430 which uses an IEEE 802.15.4 compliant communications protocol and operates in the 2.4 GHz ISM band. It is expected that other wireless systems will interfere in this band including 802.11 b/g WLAN. To avoid interference, a clear-to-send channel check is made before transmission of ranging packets. If a ranging packet becomes corrupt or is lost, the two-way transaction is disregarded and an additional transaction is made to complete the data set. To further avoid interference issues with the prototype system, testing is carried out in remote locations where interference sources are minimal.

During the process of ranging in a network of an arbitrary number of nodes, the collision of ranging and data packets may be avoided by either performing ranging on a different RF channel to that of data transfer, using allocated time slots or by random delay between transmission of packets.

4.5. Time-of-flight error margin

MacCrady *et al* [18] define the error margin as the sum of all the variances of each time delay period of the transceiver components as a TOA ranging signal passes through them. The total time delay (T_{delay}) is a Gaussian random variable formed by summing each of the independent components and is defined by equation (8) where its variance is reduced by N two-way transactions $\left(\text{i.e. } \sigma_T^2 = \sigma_{t_r}^2/N\right)$:

$$T_{\text{delay}} = \frac{1}{N}\sum_{i=1}^{N}(t_i), \qquad \text{where} \quad i = 1, 2, \ldots, N. \tag{8}$$

For a single two-way ranging transaction, the total time delay consists of a transmission and reception at the initiator and responder (with antenna delays), a relative phase offset term between device clocks and a response delay period. This is defined by equation (9), where t_{1T}, t_{2T}, t_{1R}, t_{2R} are the transmission and reception times at the initiator and responder, Δt_2 is the relative phase offset and t_{2RES} is the response period:

$$T_{\text{delay}} = t_{1T} + t_{2R} + \Delta t_2 + t_{2RES} + t_{2T} + t_{1R}. \tag{9}$$

If multiple two-way transactions are performed, then the variance in TOA estimates is expected to reduce by a root function of the number of transactions. The corresponding error margin of equation (9) is expressed by equation (10). It is clear from (10) that the error in TOA estimates can be reduced either by multiple two-way transactions or by reducing the variance in individual time components:

$$\sigma_{\text{TOA}} = \frac{1}{\sqrt{N}}[\sigma_T + \sigma_{R2} + \sigma_{\Delta t2} + \sigma_{t2RES} + \sigma_{T2} + \sigma_{1R}]. \tag{10}$$

Considering that the TI CC2430 components cannot be independently accessed to measure individual time delays, we therefore draw several assumptions based on equation (10) before proceeding: (1) the time variance from the transceiver's analogue front end for both the receiver and transmitter including antenna delays is expected to be less than 1 ns, as reported in [18]; (2) the relative phase offset between the initiator and responder will contribute to the greatest error; (3) the error contribution from the response delay will also be less than 1 ns given that the crystal oscillator accuracy is typically 40 ppm of the crystal frequency for the TI CC2430.

To verify those assumptions, figure 8 shows the capture of the SFD over successive receptions of data packets using the TI CC2420. We use the TI CC2420 in place of the TI CC2430 because of the readily available hardware and direct access to the SFD through hardware. The transmitting TI CC2420 is used as a trigger for the digital storage oscilloscope (DSO), and the SFD rising edge of the receiving TI CC2420 is captured

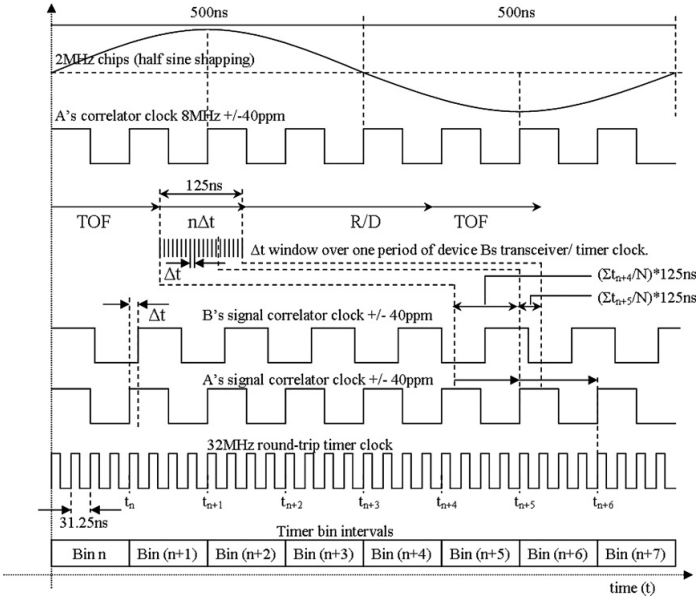


Figure 9. Two-way ranging with phase offset measurement using the TI CC2430.

by the DSO on reception of data packets; hence, figure 8 shows the variance contribution of $t_{1T} + t_{1R} + \Delta t_2$. Since t_{1T} and t_{1R} are expected to be small (i.e. < 2–3 ns), figure 8 confirms that the TI CC2420 correlates incoming chip sequences at 8 MHz (1/125 ns) given the approximate 125 ns drift period. The 140 ns period of drift is expected from t_{1T}, t_{1R} and early and late arrivals through multipath propagation during the testing in the laboratory.

Figure 9 illustrates a simplified timing diagram for the two-way ranging scheme using the TI CC2430. TOA ranging packets are transmitted using half-sine-shaped chips with frequency 2 Mchips s^{-1}. The drift period measured in figure 8 confirms the receiver's signal correlation period as 125 ns (8 MHz) in order to detect the half-sine-shaped chip sequences. To carry out round-trip timing using the TI CC2430, the MAC capture timer is used which has a frequency of 32 MHz. This is a factor of four times the correlation frequency and hence we expect the histogram bars to be separated by four clock periods for each round-trip time measurement. Although this does not affect the performance of the two-way ranging system, we expect a quantization error which will increase the number of transactions necessary to obtain a specified ranging accuracy.

Based on the result from figure 8 and the relative frequency difference between two TI CC2430 development boards, Δt is too small to measure using an oscilloscope. We make the assumption that relative phase offset between the initiator and responder is sufficiently random in order that the drift distribution can be considered normal. This corresponds to the initiator and responder having a random offset phase difference Δt. Under this assumption, ranging accuracy, in the absence of noise, is expected to be $\sigma_x^2 = 18.75/\sqrt{N}$, where N is the number of transactions (i.e. $d = vt \Rightarrow (3 \times 10^8) \cdot (125 \times 10^{-9}) = 37.5$ m, two-way $\Rightarrow 37.5/2 = 18.75$ m/clock period).

5. Preliminary experimental results

Ranging results have been obtained for LOS, NLOS and indoor environments using the standard TI CC2430 development kit operating on a single 2435 MHz channel and a transmission power of −1.5 dBm (700 mW). The LOS environment was a level grass field with no obstacles within 100.0 m of the test area. In contrast, the NLOS environment was on the University of Southampton Campus where buildings and foliage provided multipath, obstruction and signal blockage. Indoor testing was carried out in a residential flat constructed of brick work and stud-partition internal walls. Ranging was carried out over ranges of 250.0 m LOS, 120.0 m NLOS and 8.0 m indoors where the distances were restricted by boundaries of each test location.

In order to extract a valid set of ranging data, a simple program was written in Python software to interface one of the TI CC2430 development boards to a laptop computer via its RS232 port and record the ranging data. To provide initiator–responder distance referencing for the LOS and NLOS tests, an XE1610-OEMPVT GPS receiver evaluation module was also interfaced to the laptop computer via USB. The ranging measurement and GPS position estimates were then thread-read and recorded once per second each time a GPS position estimate became valid. Any corrupt samples (i.e. corrupt or lost ranging packets) were disregarded. The GPS receiver has an expected position accuracy of <5.0 m circular error probable (CEP) and resolution of >2.0 m by conversion of the

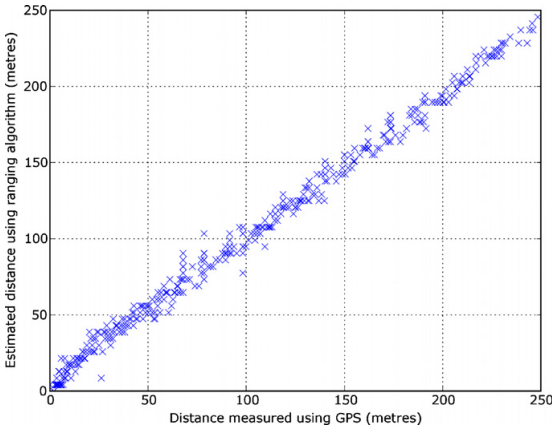


Figure 10. Performance of the ranging algorithm for the LOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 7.0 m, max error = 24.9 m, min error = 0.0 m.

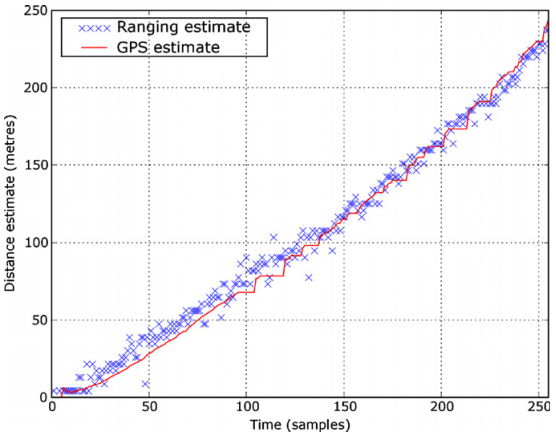


Figure 11. Performance of the ranging algorithm for the LOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

latitude and longitude coordinates to metres. To confirm our conversion calculations, a measuring wheel was also used to measure the 250.0 m for the LOS condition. The accuracy of those techniques was considered satisfactory to reference the RF two-way TOA ranging with the phase offset measurement algorithm. A 100 sample average was chosen arbitrarily per TOF measurement. This corresponds to an expected variance in ranging measurements of 1.9 m under ideal assumptions (i.e. random clock offset and in the absence of noise). Since GPS cannot obtain signal lock indoors, ranging estimates were measured in 1 m increments relative to a tape measure. A high sample set of 1000 samples were used per measurement in order to achieve an expected variance in estimates of less than 0.6 m. To calibrate the ranging measurements, the minimum round-trip period was estimated over an average of ten ranging transactions when the transceivers were in close proximity (<1.0 m). This average value was then subtracted from each ranging measurement before conversion to the distance estimate.

The linear ranging performance for the LOS condition over 250.0 m is shown in figures 10 and 11. The results confirm a typical improvement in ranging performance through averaging with an RMS error of 6.7 m. Resolution is typically 4.6 m because of the quantization introduced by averaging samples on the TI CC2430. Performance was consistent over the 250.0 m distance performance only significantly degrading on reaching the limit of the TI CC2430 radio range which is as expected. The step-response of the GPS referencing in figure 11 typically shows that the distance referencing (GPS receiver) lost signal lock during the test which introduces a small error in the measured performance. One alternative frequency-dependent RF TOA ranging method [5] reports TOA ranging estimates with the RMS error of 0.9 m_{rms} and the peak error of 2.5 m for the LOS condition using an FPGA and similar 2.4 GHz RF radio module. In comparison, our time-dependent TOA ranging results inherit greater RMS error which we expect is due to both the low

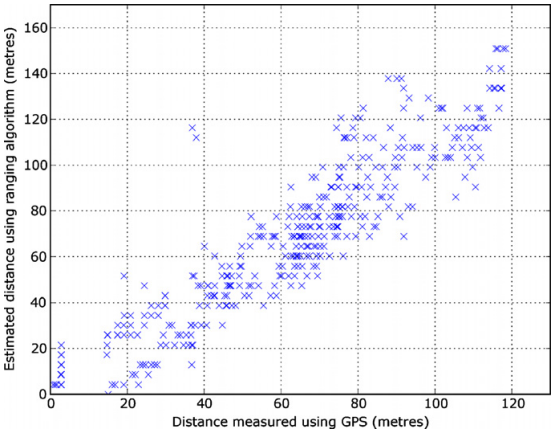


Figure 12. Performance of the ranging algorithm for the NLOS condition, TI CC2430 ranging estimate versus GPS measured distance, 100 two-way samples. RMS error = 15.8 m, max error = 79.5 m, min error = 0.0 m.

averaged sample number and the inaccurately generated period Δt and unknown synchronization period using our prototype system implemented on off-the-shelf hardware.

Performance for the NLOS condition over 120.0 m is shown in figures 12 and 13 by moving the responder through different LOS, NLOS and complete signal blocked positions. The increased spread in ranging estimates illustrated in figure 12 confirms that the ranging system suffers more significantly in those conditions as expected. The RMS error is 15.8 m which is over twice the error reported for the LOS condition. This is expected not only for the aforementioned reason, but also due to the loss of GPS signal lock and the contoured landscape which was not accounted for with reference to GPS. NLOS ranging in [5] reports ranging results through a wall for fixed distance up to 10 m. The ranging error is 1.8 m_{rms} with a peak error of 3.4 m. We expect that the

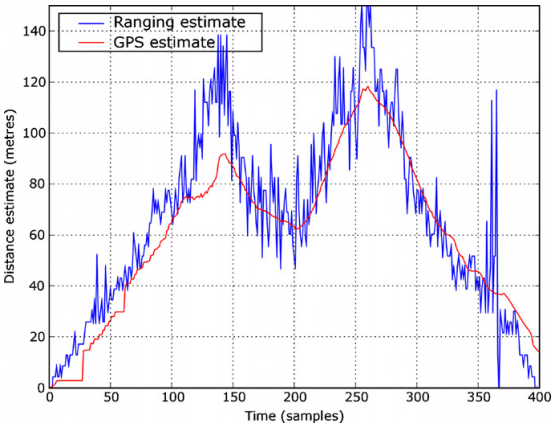


Figure 13. Performance of the ranging algorithm for the NLOS condition, TI CC2430 ranging estimate and GPS measured distance versus time (samples), 100 two-way samples.

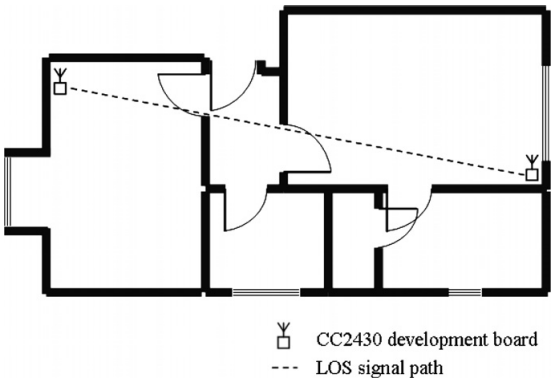


Figure 14. Scale diagram of the residential flat used for indoor testing of the two-way TOA ranging algorithm. External walls constructed using brickwork; internal walls are stud-partition. Ranging experiments conducted for the LOS condition over 8 m with internal doors open.

significantly larger range error in this result is due to the larger transceiver–transceiver separation distance and NLOS signal propagation over the NLOS test environment.

A scale drawing of the indoor test environment is illustrated in figure 14. The initiator–responder separation distances are increased in 1 m increments over a total distance of 8 m with each estimate being computed for 1000 averaged samples. The sample number is increased to reduce the variance in estimates due to the short testing distance. Internal doors were left open during the test and testing was carried out for the LOS condition through three rooms including a living room, hall and bedroom with full furnishings including tables, bookshelves, chairs, glass units and many other surfaces which contribute to signal distortion and scattering. Figure 15 illustrates ranging performance for the condition where the responder is placed at each known distance between 0.0 and 8.0 m. The ranging RMS error was measured as 1.7 m

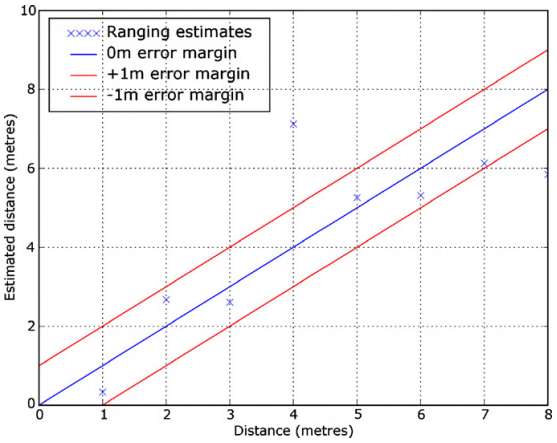


Figure 15. Performance of the ranging algorithm for the indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 1.7 m, max error = 3.2 m, min error = 0.3 m.

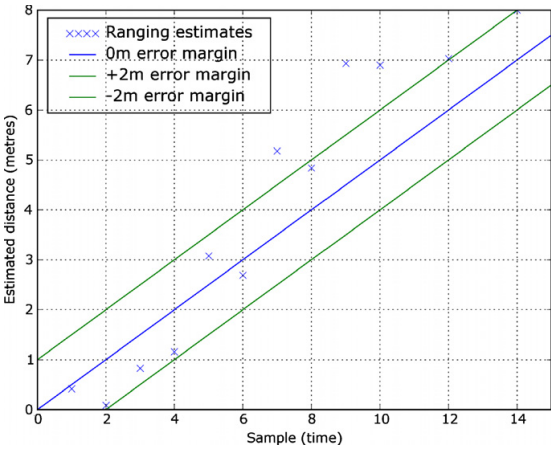


Figure 16. Real-time motion performance of the ranging algorithm for indoor condition, TI CC2430 ranging estimate versus measured distance, 1000 two-way samples. RMS error = 3.2 m, max error = 6.0 m, min error = 0.0 m.

with a maximum error of 3.2 m. This compares well to the indoor LOS results reported in [5] where the ranging error was measured as 2.6 m_{rms} with a peak error of 5.5 m over similar transceiver–transceiver test distances. Our results confirm that averaging greater sample numbers reduces TOA range estimates as expected. Figure 16 shows the performance of the algorithm for real-time motion when the responder is linearly moved over an initiator–responder distance of 8.0 m. The RMS error was measured as 3.2 m with a maximum error of 6.0 m. The larger error was expected under velocity because of the time-variant channel.

The results are summarized in table 1. Ranging accuracy is constrained by noise, quantization in the round-trip timing measurements and averaged sample number. Assuming a

Table 1. Prototype ranging system estimation errors (m) measured relative to the GPS range estimate.

	Sample no	σ expected	RMS error (m)	Max. error (m)
LOS	100	$\approx 1.9 + \sigma_n$	7.0	24.9
NLOS	100	$\approx 1.9 + \sigma_n$	15.8	79.5
Indoor	1000	$\approx 0.6 + \sigma_n$	1.7	3.2

normally distributed clock offset (figure 8), the expected accuracies in the absence of noise, transceiver AFE and signal lock delays are 1.9 m for the LOS and NLOS conditions using a 100 sample average ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 100$). Under the same assumptions, indoor accuracy was expected within 0.6 m using 1000 averaged samples ($\sigma_x^2 = 18.75/\sqrt{N}$, where $N = 1000$). The addition of noise, signal multipath, AFE and transceiver signal lock delays increased this variance for each condition. Figure 8 confirms a 140 ns relative drift period; hence, we expect the variance in time delay from all additional contributions to be in the region 0–10 ns (140 ns − 125 ns → 15 ns, minus multipath delay from test environment), hence limiting the performance of this ranging technique. We expect those time variance contributions to be reduced by increasing the number of two-way ranging transactions.

6. Conclusion

We have successfully implemented and demonstrated a novel narrow-band two-way TOA ranging method with phase offset measurement using low-frequency clocks to determine range measurements with accuracies better than 7.0 m LOS, 15.8 m NLOS and 1.7 m indoor using low-cost, low-power hardware. In addition, our algorithm operates fully on a single-chip solution. To the best of the authors' knowledge, this is the first time-dependent RF TOA ranging scheme to exploit the relative offset in frequency between two radio transceivers involved with TOA ranging in order to improve ranging resolution. The technique therefore has substantial benefits in WSNs where sensor nodes are required to operate with low-power consumption and thus a low system clock frequency. In addition, the use of conventional RF as opposed to UWB allows the operating range of the WSN within regulation to be over a much greater range (>50 m).

The resolution of this technique is bound by three fundamental factors: (1) variance in time delays of the transceiver analogue front end; (2) the distribution of the relative clock offset between the transceivers herein assumed to be normally distributed; (3) the signal-to-noise-ratio (SNR). The time taken to achieve a specified degree of accuracy is limited by the bandwidth of the signal correlator.

For this technique to operate as expected, the assumption was made that the distribution of the relative clock offset between transceivers is normally distributed. Figure 17 illustrates the quantized distribution of the relative clock offset. This test was performed for 1000 round-trip TOA measurements where the initiator and responder were placed with antennas separated by 0.1 m. The signal correlator

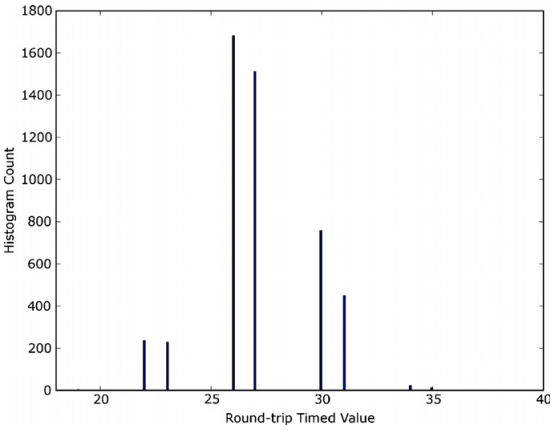


Figure 17. Histogram count of round-trip timed values for 5000 two-way TOA measurements using the TI CC2430.

frequency was determined as 8 MHz, four times lower than the 32 MHz MAC timer used for round-trip timing; hence, we expect histogram bars to be spaced by four clock periods (i.e. at 22, 26, 30 and 34). The additional bars at 23, 27, 31 and 35 we expect are caused by late triggering of the capture timer. In the ideal case (i.e. in the absence of noise and no time delays in AFE) only two histogram bars exist; however, the additional bars are expected due to the 140 ns drift period shown in figure 8. It is expected that error is also caused by the non-ideal receiver lock on chip-sequences during reception as the receiver tries to synchronize to the packet preamble chip sequence.

We suspect that the recorded variances are greater than expected because of the error contribution caused by referencing the system to GPS during the test. In addition, we expect the error to exist in the calibration because the relative phase offset between the device clocks will not be the ideal normal distribution that we assume.

One previous RF TOF ranging system (frequency-dependent) prototyped by Karalar and Rabaey [4] reports an RF TOA ranging scheme with estimation accuracy within −0.5 to 2.0 m using an FPGA with a 100 Msps ADC sample rate. Ranging accuracy in this scheme is improved by increasing the sample rates of the signal ADC and DAC. We use a TI CC2430 with determined signal sampling of 8 Msps and a TOA phase offset scheme to achieve ranging accuracy below 7.0 m RMS under LOS conditions using 100 averaged samples. Ranging accuracy is improved by increasing the sample number making this scheme suitable for WSN applications where low-frequency system clocks are ideal.

Our further work will involve improving the accuracy and resolution of this TOA-based ranging technique and implementing the method into fixed infrastructure and relative locationing systems. We intend to improve the performance by using a known frequency difference between the transceivers in order to obtain Δt more accurately. This will enable us to achieve our desired accuracy with significantly less round-trip samples. We also intend to replace the arbitrary chosen sample number N by considering the variance in the

round-trip time measurement distribution to automatically perform the required number of ranging transactions N for a specified ranging accuracy. Further development will involve the implementation of filtering to reduce the variance of round-trip measurements under NLOS conditions. We also intend to investigate further the transceiver signal lock to reduce the error in round-trip measurements.

References

[1] Mainwaring A, Polastre J, Szewczyk R, Culler D and Anderson J 2002 Wireless sensor networks for habitat monitoring *WSNA'02: Proc. 1st ACM Int. Workshop on Wireless Sensor Networks and Applications*

[2] Tian J, Wu H and Gao M 2008 Measurement and control system of sewage treatment based on wireless sensor networks *IEEE Int. Conf. on Industrial Technology, 2008: ICIT 2008 (April 2008)* pp 1–4

[3] Fontana R J, Richley E and Barney J 2003 Commercialization of an ultra wideband precision asset location system *IEEE Conf. on Ultra Wideband Systems and Technologies, 2003 (16–19 November 2003)* pp 369–73

[4] Karalar T C and Rabaey J 2006 An RF ToF based ranging implementation for sensor networks *IEEE Int. Communications Conf. (University of California, Berkeley, June 2006)* vol 7, pp 3347–52

[5] Lanzisera S, Lin D T and Pister K S J 2006 RF time of flight ranging for wireless sensor network localization *Int. Workshop on Intelligent Solutions in Embedded Systems, 2006 (30 June 2006)* pp 1–12

[6] Fontana R J and Gunderson S J 2002 Ultra-wideband precision asset location system *IEEE Conf. on Ultra Wideband Systems and Technologies (May 2002)* pp 147–50

[7] Li X 2005 Performance study of RSS-based location estimation techniques for wireless sensor networks *Military Communications Conf., 2005: MILCOM 2005 (IEEE, 17–20 October 2005)* vol 2, pp 1064–8

[8] Schantz H G 2007 A real-time location system using near-field electromagnetic ranging *Antennas and Propagation Society Int. Symp., 2007 (IEEE, 9–15 June 2007)* pp 3792–5

[9] Peng R and Sichitiu M L 2006 Angle of arrival localization for wireless sensor networks *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (28 September 2006)* pp 374–82

[10] Texas Instruments TI CC2430 datasheet, www.ti.com

[11] Urkowitz H 1983 *Signal Theory and Random Processes* (Boston, MA: Artech House)

[12] Chung W C and Ha D S 2003 An accurate ultra wideband (UWB) ranging for precision asset locationing *IEEE Conf. on Ultra Wideband Systems and Technologies (16–19 November 2003)* pp 389–93

[13] Xia T, Zheng H, Li J and Ginawi A 2005 Self-refereed on-chip jitter measurement circuit using Vernier oscillators *IEEE Computer Society Annual Symp. on VLSI (May 2005)* pp 218–23

[14] Sallai J, Balogh G, Maróti M, Lédeczi A and Kusy B 2004 Acoustic ranging in resource-constrained sensor networks *Int. Conf. on Wireless Networks (Nov. 2004)* p 467

[15] Xia T, Zheng H, Li J and Ginawi A 1989 Fundamentals of two-way time transfers by satellite *Proc. 43rd Ann. Symp. on Frequency Control (May–June 1989)* pp 174–8

[16] TI/Chipcon CC2430DK Development Kit, www.ti.com

[17] IEEE 2003 802.15.4 Standard for Information Technology (London: IEEE)

[18] McCrady D D, Doyle L, Forstrom H, Dempsey T and Martorana M 2000 Mobile ranging using low-accuracy clocks *IEEE Trans. Microwave Theory Techn.* **48** 951–8

Glossary

Accuracy	Defines the difference between the true distance and the estimated distance of the measurement
Attenuation	the reduction in the strength of a signal
Azimuth	The horizontal angular distance from a reference direction
Bandwidth	A measure of the width of a range of frequencies or the rate of data transfer
Bearing	Angular direction measured from one position to another with respect to a reference direction
Blind	A device with no prior knowledge of its position
Calibration	The act of checking or adjusting the accuracy of a measuring instrument by comparison with a standard
Correlation	The simultaneous change in value of two numerically valued random variables
Doppler effect	The observed frequency of a wave when the transmitter and receiver are in motion relative to each other. Frequency increases when the transmitter receiver distance decreases and increases when the transmitter receiver distance increases
Doppler shift	The change in the observed frequency of a wave due to Doppler effect
Initiator	The device which 'initiates' the ranging process

Localization	The process of estimating the position of a device in relation to a some referencing architecture
Locate	To determine or specify the position or limits of a device
Location	An estimate of the position of where a sensor node could be
Multipath	A signal that takes two or more paths because the signal is reflected or diffracted off surfaces or obsticles
Narrow-band	The bandwidth of the signal does not significantly exceed the channel's coherence bandwidth
Node	An individual sensing device within a wirless sensor network
Optimizer	algorithm or process to increase computing speed and efficiency
Orientation	Defined as a fixed direction against which an angle is measured in a clockwise direction from north
Preamble	A unique string of integer values used to identify elementary streams of strings in an RF transmitter-receiver system
Pseudorandom	A random sequence of bits generated by a definite, nonrandom computational process
Pseudorange	A first-approximation measurement for the distance between two points which includes both ranging information and timing offset
Quantization	To limit the possible values to a discrete set of values
Ranging	The estimate of the distance to a remote point (target) from a known observation point is known as ranging
Reference	A device with prior knowledge of its position

Resolution	Defines the smallest change in distance that can be detected by the system
Responder	The device that responds or reflects the ranging message back to the 'initiator'
Shadowing	Attenuation of the direct-path signal resulting from obstructing obstacles
Spread Spectrum	A technique by which a signal to be transmitted is modulated onto a pseudo-random, noise-like, wideband carrier signal, producing a transmission with a much larger bandwidth that that of the date modulation
Start of Frame Delimiter	A unique integer value used to identify the start of data in an elementary stream of integers
Synchronization	Occur simultaneously or operate with exact coincidence in time
Transceiver	A device that both transmits and receives analog or digital signals
Triangulation	To determine the location of an unknown position by the use of angle measurements from two or more references
Trilateration	To determine the location by use of distance measurements from two or more references
Ubiquitous	Having or seeming to have the ability to be everywhere at once
Ultra-wideband	A signal operating with transmission bandwidth greater than 500 MHz

Bibliography

[1] Mark Weiser. The world is not a desktop. *interactions*, 1(1):7–8, 1994.

[2] M. Weiser. Ubiquitous computing. *Computer*, 26(10):71–72, 1993.

[3] Mark Weiser. Some computer science issues in ubiquitous computing. *Commun. ACM*, 36(7):75–84, 1993.

[4] Mark Weiser. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, 3(3):3–11, 1999.

[5] Adam Greenfield. *Everyware: The Dawning Age of Ubiquitous Computing*. Peachpit Press, Berkeley, CA, USA, 2006.

[6] Uwe Hansmann, Lothar Merk, Martin S. Nicklous, and Thomas Stober. *Pervasive Computing: The Mobile World*. Springer-Verlag, Berlin, Germany, 2nd edition, August 2003.

[7] J. Blumenthal, M. Handy, F. Golatowski, M. Haase, and D. Timmermann. Wireless sensor networks - new challenges in software engineering. *Emerging Technologies and Factory Automation, 2003. Proceedings. ETFA '03. IEEE Conference*, 1:551–556 vol.1, Sept. 2003.

[8] David Culler, Deborah Estrin, and Mani Srivastava. Guest editors' introduction: Overview of sensor networks. *Computer*, 37(8):41–49, 2004.

[9] S. Vardhan, M. Wilczynski, G.J. Portie, and W.J. Kaiser. Wireless integrated network sensors (wins): distributed in situ sensing for mission and flight systems. In *Aerospace Conference Proceedings, 2000 IEEE*, volume 7, pages 459–463 vol.7, 2000.

[10] Doug Steel. Smart dust, 2005.

[11] Kevin A. delin. The sensor web: A distributed, wireless monitoring system, 2004.

[12] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM.

[13] R.J. Fontana and S.J. Gunderson. Ultra-wideband precision asset location system. pages 147–150, 2002.

[14] Liyang Yu, Neng Wang, and Xiaoqiao Meng. Real-time forest fire detection with wireless sensor networks. In *Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on*, volume 2, pages 1214–1217, Sept. 2005.

[15] Eng-Han Ng, Su-Lim Tan, and J.G. Guzman. Road traffic monitoring using a wireless vehicle sensor network. In *Intelligent Signal Processing and Communications Systems, 2008. ISPACS 2008. International Symposium on*, pages 1–4, Feb. 2009.

[16] R.J. Fontana. Recent system applications of short-pulse ultra-wideband (uwb) technology. *Microwave Theory and Techniques, IEEE Transactions on*, 52(9):2087–2104, Sept. 2004.

[17] T.C. Karalar and J. Rabaey. An rf tof based ranging implementation for sensor networks. volume 7, pages 3347–3352, June 2006.

[18] E. D. Kaplan and C. J. Hegarty. *Understanding GPS Principles and Applications, Second Edition*. Artech House, 46 Gillingham Street, London, 2006.

[19] RF Solutions. Xe1610-oempvt gps receiver, reference design 2.0, 2003.

[20] Chipcon. Cc2431dk development kit, 2006.

[21] R.J. Fontana, E. Richley, and J. Barney. Commercialization of an ultra wideband precision asset location system. pages 369–373, Nov. 2003.

[22] Ubisense. Ubisense limited website, 2005.

[23] Inc Multispectral Solutions. Pal650 ultra wideband precision asset location system evaluation kit. Description of pal650 UWB locationing system, August 2004.

[24] R. Zetik A. Ward D. Porcino, J. Sachs. *Uwb Communications Systems: A Comprehensive Overview*. Hindawi Publishing Corporation, 2006.

[25] L. Berti N. R. Harris N. M. White B. M. Al-Hashimi G. V. Merritt, A. S. Weddell. A wireless sensor network for cleanroom monitoring.

[26] S. Lanzisera, D.T. Lin, and K.S.J. Pister. Rf time of flight ranging for wireless sensor network localization. pages 1–12, June 2006.

[27] F.L.Lewis. Wireless sensor networks, 2004.

[28] Jon S. Wilson. *Sensor Technology Handbook*. Elsevier, Linacre House, Jordan Hill, Oxford OX2 8DP, UK, 2005.

[29] Ieee 802.15.4 standard for information technology, October 2003.

[30] Diane Cook and Sajal Das. *Smart Environments: Technology, Protocols and Applications (Wiley Series on Parallel and Distributed Computing)*. Wiley-Interscience, 2004.

[31] J. Wiczer S. Woods R. Johnson, K. Lee. A standard smart transducer interface - ieee 1451, 2001.

[32] The sensor network musium, 2010.

[33] Chipcon. Cc2430dk development kit, 2006.

[34] Ciarn Lynch. Processor choice for wireless sensor networks. In *in REALWSN05: Workshop on Real-World Wireless Sensor Networks*, pages 1–5, 2005.

[35] ZigBee Alliance. Zigbee. http://www.zigbee.org/, Jan 2010.

[36] S. C. Ergen. Zigbee/ieee 802.15.4 summary, September 2004.

[37] K. T. Le. Zigbee system-on-chip (soc) design. High Frequency Electronics, 2006.

[38] M. Banan M. Taylor, W. Waung. *Internetwork Mobility: The CDPD Approach*. Prentice Hall, 1996.

[39] Bluetooth special interest group. Bluetooth. http://www.bluetooth.com/, Jan 2010.

[40] W.Kang K. S. Kwak, W. Zhang. Ultra-wideband ranging method and system using narrowband interference supression waveform, January 2009.

[41] C. Savarese, J.M. Rabaey, and J. Beutel. Locationing in distributed ad-hoc wireless sensor networks. *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, 4:2037–2040 vol.4, 2001.

[42] Xiang Ji and Hongyuan Zha. Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling. *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 4:2652–2661 vol.4, March 2004.

[43] M. Rydstrom, A. Urruela, E. Strom, and A. Svensson. Low complexity tracking for ad-hoc automotive sensor networks. pages 585–591, Oct. 2004.

[44] B. Sklar. *Digital Communications Fundamentals and Applications*. Prentice Hall, Prentice Hall International (UK) Ltd, 1988.

[45] M. Maroti A. Ledeczi B. Kusy J. Sallai, G. Balogh. Acoustic ranging in resource-constrained sensor networks.

[46] H. Schantz. Near field ranging algorithm, August 2004.

[47] M. Nelkon. *Advanced Level Physics, 7th Edition*. Heinemann Educational Publishers, Halley Court, Jordan Hill, Oxford OX2 8EJ, 1997.

[48] W. R. Phillips I. S. Grant. *Electromagnetism, second edition.* John Wiley and Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2004.

[49] Qicai Shi, N. Correal, S. Kyperountas, and Feng Niu. Performance comparision between toa ranging technologies and rssi ranging technologies for multi-hop wireless networks. volume 1, pages 434–438, Sept., 2005.

[50] Jeffrey H. Reed. *An Introduction to Ultra Wideband Communication Systems.* Prentice Hall, Pearson Education, Inc. One Lake Street, Upper Saddle River, NJ 07458, 2005.

[51] Yilin Zhao. Mobile phone location determination and its impact on intelligent transportation systems. *Intelligent Transportation Systems, IEEE Transactions on*, 1(1):55–64, Mar 2000.

[52] Xinrong Li. Performance study of rss-based location estimation techniques for wireless sensor networks. pages 1064–1068 Vol. 2, Oct. 2005.

[53] G.I. Wassi, C. Despins, D. Grenier, and C. Nerguizian. Indoor location using received signal strength of ieee 802.11b access point. pages 1367–1370, May 2005.

[54] T. Locher, R. Wattenhofer, and A. Zollinger. Received-signal-strength-based logical positioning resilient to signal fluctuation. pages 396–402, May 2005.

[55] Chipcon. Chipcon cc2430 datasheet, 2006.

[56] D. Gore A. Paulraj, R. Nabar. *Introduction to Space-Time Wireless Communications.* Cambridge University Press, The Pitt Building, Trumpington Street, Cambridge, United Kingdom, 2006.

[57] A. Goldsmiths. *Wireless Communications.* Cambridge University Press, 40 West 20th street, New York, NY 10011-4211, USA, 2005.

[58] N. Patwari, R.J. O'Dea, and Yanwei Wang. Relative location in wireless networks. *Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd*, 2:1149–1153 vol.2, 2001.

[59] H.G. Schantz. A real-time location system using near-field electromagnetic ranging. pages 3792–3795, June 2007.

[60] D. Tholl and M. Fattouche. Angle of arrival analysis of the indoor radio propagation channel. volume 1, pages 79–83 vol.1, Oct 1993.

[61] Z. Popovic, C. Walsh, P. Matyas, C. Dietlein, and D.Z. Anderson. High-resolution small-aperture angle of arrival detection using nonlinear analog processing. volume 3, pages 1749–1752 Vol.3, June 2004.

[62] P Rong and M.L. Sichitiu. Angle of arrival localization for wireless sensor networks. volume 1, pages 374–382, Sept. 2006.

[63] S.M. Lanzisera. Rf ranging for location awareness, 2009.

[64] S. Srirangarajan and A.H. Tewfik. Localization in wireless sensor networks under non line-of-sight propagation. *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, 6:5 pp.–, Nov.-2 Dec. 2005.

[65] A. Tian Xia; Hao Zheng; Jing Li; Ginawi. Self-refereed on-chip jitter measurement circuit using vernier oscillators. pages 218–223. IEEE Computer Society Annual Symposium on VLSI, May 2005.

[66] T. H. Lee. *The Design of CMOS Radio-Frequency Intergrated Circuits*. Cambirdge University Press, 40 West 20th Street, New York, NY 10011-4211, USA, 2004.

[67] H. Urkowitz. *Signal Theory and Random Processes*. Artech House, 1983.

[68] D. S. Ha W. C. Chung. An accurate ultra wideband (uwb) ranging for precision asset locationing. pages 389– 393. IEEE Conference on Ultra Wideband Systems and Technologies, 16.

[69] C.L. Bennett and G.F. Ross. Time-domain electromagnetics and its applications. *Proceedings of the IEEE*, 66(3):299–318, March 1978.

[70] D.W. Hanson. Fundamentals of two-way time transfers by satellite. *Frequency Control, 1989., Proceedings of the 43rd Annual Symposium on*, pages 174–178, May-2 Jun 1989.

[71] Bell Labs Lucent Technologies. Wise design of indoor and outdoor wireless systems. http://www.bell-labs.com/org/wireless/wisext.html, 2002.

[72] Wireless Global Technologies. Celplanner. http://www.celplan.com/, 2010.

[73] J. Holtzman M. P. Wylie. The non-line of sight problem in mobile location estimation. volume 2, pages 827– 831. 5th IEEE Int. Conf. Universal Personal Communications, 1996.

[74] D.D. McCrady, L. Doyle, H. Forstrom, T. Dempsey, and M. Martorana. Mobile ranging using low-accuracy clocks. *Microwave Theory and Techniques, IEEE Transactions on*, 48(6):951–958, Jun 2000.

[75] J.V. Hatfield P. Dudek, S. Szczepanski. A high resolution cmos time-to-digital converter utilizing a vernier delay line. volume 35, pages 240–247. IEEE Transcation on Solid-State Circuits, February 2000.

[76] A. Ivanov S. Tabatabaei. Embedded timing analysis: A soc infrastructure. volume 19, pages 24–36. IEEE Design and Test of Computers, 2002.

[77] IAR systems.

[78] N. Reijers K. Langendoen. Distributed localization in wireless sensor networks: a quantitative comparison.

[79] E. Al M. Gabriella, D. Benedetto. *UWB Communication Systems: A Comprehensive Overview*. Hindawi Publishing Corporation, 2006.

[80] Crossbow. Crossbow website, 2010.

[81] M.P. Wylie-Green and S.S. Wang. Robust range estimation in the presence of the non-line-of-sight error. volume 1, pages 101–105 vol.1, 2001.

[82] J.A. Gibbs. Demodulation of convolutionally encoded ffh mfsk in jamming, multiple access and frequency varying channels.