UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATION ENGINEERING

Faheem Ahmed

IMPROVING RSSI BASED DISTANCE ESTIMATION FOR WIRELESS SENSOR NETWORKS — A STATISTICAL ANALYSIS

Master´s thesis for the degree of Master of Science in Technology submitted for inspection in Vaasa, 1st of October, 2010.

Supervisor	D.Sc. (Tech) Mohammed Elmusrati
Instructor	M.Sc. (Tech) Reino Virrankoski

ACKNOWLEDGMENTS

First I like to thank Professor Mohammed Elmusrati and Lecturer Reino Virrankoski for their guidance and support leading me to the completion of this Master's Thesis. I also appreciate the cooperation and support of Laboratory Engineer Veli-Matti Eskonen and Laboratory Engineer Juha Miettinen who provided necessary equipment and a nice working environment to complete this thesis. I am especially grateful to my colleague Niklas Wiik for his valuable help. I also like to thank everyone else who contributed and helped in any manner leading to the completion of this thesis.

Faheem Ahmed

1st of October 2010.

TABLE OF CONTENTS

SYMBOLS AND ABBREVIATIONS

6LoWPAN	IPv6-based Low-power Wireless Personal Area Networks
AOA	Angle of Arrival
API	Application Programming Interface
CPU	Central Processing Unit
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
FFD	Full Function Device
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISM	Industry, Scientific and Medical
ISO	International Organization for Standardization
MAC	Medium Access Control
OS	Operating System
OSI	Open System Interconnection
PAN	Personal Area Network
PC	Personal Computer
PHY	Physical
PiccSIM	Platform for Integrated Communications and Control Design, Simulation, Implementation and Modeling
QoT	Quality of Trilateration
RF	Radio Frequency
RFC	Request For Comments
RFD	Reduced Function Device
RSS	Received Signal Strength
RSSI	Received Signal Strength Identifier
RTOS	Real Time Operating System
SD	Standard Deviation

SoC	System on Chip
TCP	Transmission Control Protocol
TDOA	Time Difference of Arrival
TOA	Time of Arrival
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

UNIVERSITY OF VAASA
Faculty of Technology

Author:	Faheem Ahmed
Topic of the Thesis:	Improving RSSI Based Distance Estimation for Wireless Sensor Networks—A Statistical Analysis
Supervisor:	Mohammed Elmusrati
Instructor:	Reino Virrankoski
Degree:	Master of Science in Technology
Department:	Department of Computer Science
Degree Program:	Degree Program in Telecommunication Engineering
Major of Subject:	Telecommunication Engineering
Year of Entering the University:	2006
Year of Completing the Thesis:	2010 **Pages: 59**

ABSTRACT

In modern everyday life we see gradually increasing number of wireless sensor devices. In some cases it is necessary to know the accurate location of the devices. Most of the usual techniques developed to get this information require a lot of resources (power, bandwidth, computation, extra hardware) which small embedded devices cannot afford. Therefore techniques, using small resources without the need for extra hardware, need to be developed. Wireless sensor networks are often used inside buildings. In such environment satellite positioning is not available. As a consequence, the location computation must be done in network-based manner.

In this thesis a received signal strength indicator (RSSI) based distance estimation technique for 802.15.4 network based on CC2431 radio is discussed. In this approach we try to differentiate between good and erroneous measurements by imposing limits based on standard deviation of RSSI and the number of lost packets. These limits are included as a part of the model parameter estimation process. These limits are optimized in order to improve the resulting distance estimates with minimum loss of connectivity information. We experimentally evaluated the merits of the proposed method and found it to be useful under certain circumstances.

KEYWORDS: Wireless Sensor Networks, Localization, Distance Estimation, RSSI, IEEE 802.15.4.

1. INTRODUCTION

Wireless sensor networks (WSN) have been receiving a lot of attention recently due to a wide range of potential applications such as environment monitoring, warehouse inventory, object tracking etc. Typically a WSN is expected to consist of a large number of small sensor devices deployed over wide area. The sensor devices called sensor nodes or sensor motes have very limited recourses in terms of power, memory, radio range, and processing capabilities.

In this thesis a wireless sensor network has been investigated and tested for improved localization for both indoor and outdoor environments. Since the sensor nodes are equipped with microcontrollers and memory, data sensed by the nodes can partially be processed locally. The model parameter calculation is done in centralized manner in pc after collecting the data from the network. The main goal was to find a way to improve distance estimates for an 802.15.4 WSN based on received signal strength measurements.

The rest of the thesis is organized as follows. Chapter two discusses different network protocols and their functionality and integration with each other. In chapter three the properties of radio path are discussed. Chapter four describes basics of distance based localization and related challenges. In chapter five detailed description of the related hardware system is discussed. In chapter six the software architecture and the developed applications are discussed. Chapter seven describes the experimental setup for outdoor and indoor measurements. In chapter eight the results are discussed and analyzed.

2. BASICS OF NETWORKS

Modern day networking solutions often require us to integrate different communication systems with each other. In this chapter we briefly discuss about the basic theory of network systems.

2.1. OSI Model

The Open System Interconnection Model (OSI) defined by International Organization for Standardization (ISO) serves as a reference for understanding different network protocol stacks. OSI model is a stack of seven layers as described in Figure 1. Each layer is basically a collection of functions which provide similar services to the upper layer. Each layer can be developed independently. Similar layers on two different open systems are interconnected by specific protocols (ISO 7498 1994; Stallings 2007: 42-45).

The application layer is the user’s access point to the OSI environment. It also provides distributed information services. The presentation layer deals with the syntax and representation of the information transferred between application processes so that the application process does not have to deal with common representation of information. The session layer provides the means necessary to cooperate, organize and synchronize dialogues between presentation entities and to establish and release a connection in orderly manner. The transport layer ensures reliable and transparent transfer of data between session-entities so that they do not have to deal with the ways to achieve reliable and cost effective transfer of data. The network layer provides routing and relay services to the transport entities. The Data Link Layer enables network entities to transfer data reliably and detect and possibly correct any errors occurred in the Physical Layer. The Physical Layer deals with the ways necessary for activating, maintaining, and de-activating physical connections between data link entities (Stallings 43; ISO 7498 1994: 32-52).

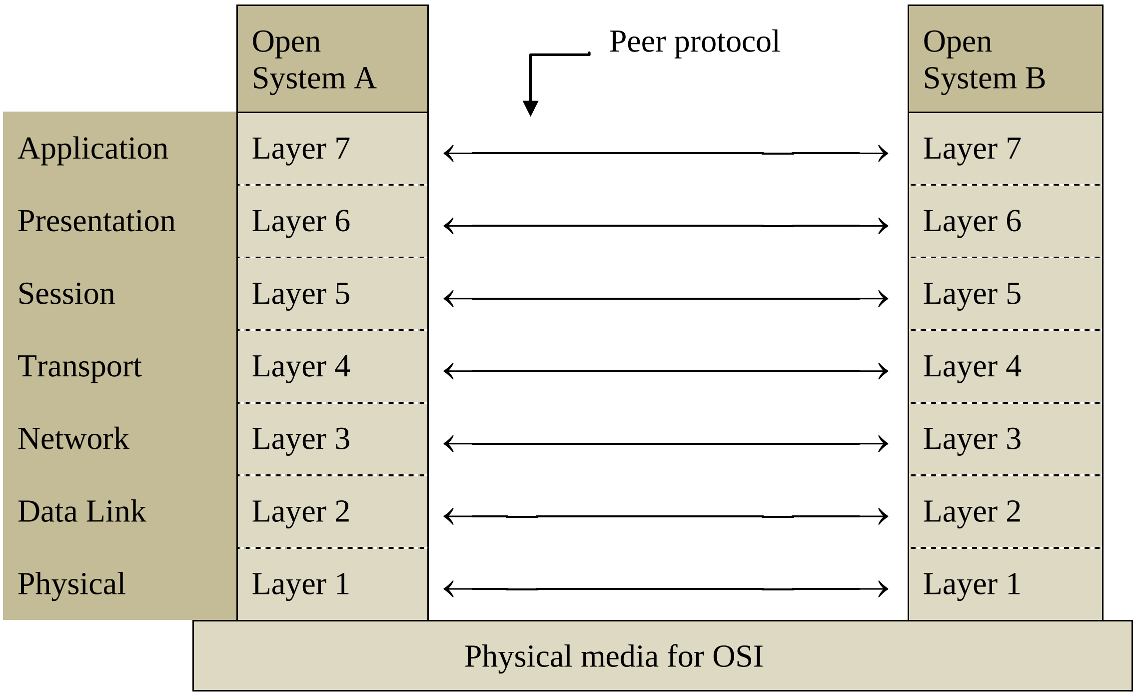

Figure 1. Structure of OSI model (ISO 7498 1994: 28).

In practice, the OSI model serves as a theoretical reference for several protocol stacks. The Internet Protocol Suite (TCP/IP) consist of link layer, IP layer, transport layer (RFC 1122) and the Application layer with support protocols (RFC 1123). In literature TCP/IP is usually divided into five layers in comparison to OSI model (Stallings 2007:34-44). The five layered structure is described in Figure 2.

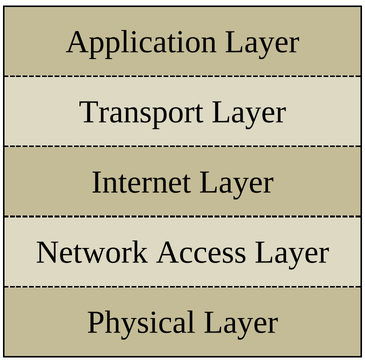

Figure 2. Structure of TCP/IP protocol suit (Stallings 2007:44).

2.2. TCP

Transmission Control Protocol (TCP) provides reliable connection to transfer data stream between programs running on two networked devices. It also provides control over segment size, network congestion and flow control. TCP only supports unicast communications. TCP connections are not suitable for very short transactions, as in case of WSNs. (RFC793 1981.)

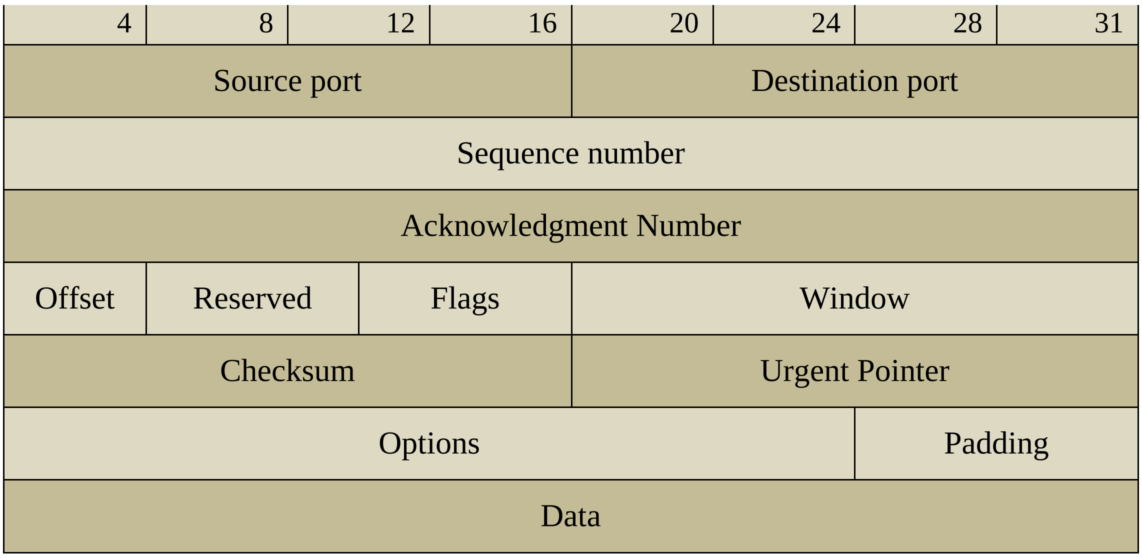

Figure 3. TCP Header Format.

TCP header as illustrated in Figure 3 contains 16 bit source address and 16 bit destination address. The address field is followed by 32 bit sequence number and acknowledgment number. 4 bit data offset specifies the size of TCP header. The minimum size is 5 word or 20 bytes and maximum size is 15 word or 60 byte. The Reserved 4 bits are for future use and are always set to zero. The 8 bits flags are also called as control bits. The window size specifies the number of bytes that receiver can receive. Checksum field is used for error checking. It is followed by the urgent pointer. Options field is of variable size (0 to 320 bits). Its length is determined by the data offset field.

2.3. UDP

The User Datagram Protocol (UDP) uses a simple transmission model without implicit hand-shaking dialogues for guaranteeing reliability, ordering, or data. Thus, UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP is compatible with packet broadcasting and multicasting without requiring much overhead, which makes it suitable for certain applications in WSNs (Postel 1980).

4	8	12	16	20	24	28	31
Source port				Destination port			
Length				Checksum			
Data Octets …							

Figure 4. User Datagram Header Format.

UDP header as illustrated in Figure 4 contains 16 bit fields for source and destination port numbers. The length field specifies the length of the datagram in bytes. The minimum length is 8 byte and the theoretical maximum is 65535 bytes while the practical maximum is 65507 bytes. The checksum field is used for checking errors in header and data (Forouzan 2000).

2.4. ICMP

The Internet Control Message Protocol (ICMP) is used to send an error report message from a gateway or destination host to a source host, concerning an error in datagram processing. It relies on basic support of IP for the transmission of ICMP message. (RFC 792 1981; Stallings 2007: 582-583.)

<table>
<tr><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td><td>24</td><td>28</td><td>31</td></tr>
<tr><td colspan="2">Type</td><td colspan="2">Code</td><td colspan="4">Checksum</td></tr>
<tr><td colspan="8">(depends on message type)</td></tr>
<tr><td colspan="8">(depends on message type)</td></tr>
</table>

Figure 5. ICMP error message format.

In Figure 5 the type defines one of the sixteen different error messages (RFC 792 1981). The next generation ICMPv6, which requires IPv6 header, is defined in IETF publication (RFC 2463 (1998). It is used to communicate control messages between IPv6 nodes.

2.5. IPv4

Internet Protocol version 4 (IPv4) is described in IETF publication (RFC 7911981). It is a part of the TCP/IP suit. It provides connectionless communication between end systems which enables the service to be flexible and robust. The system operates on best-effort delivery model. It does not guarantee delivery, proper sequencing or duplicate delivery avoidance. To enable these aspects an upper layer transport protocol is used along with IP, e.g. TCP (Stallings 2007:569-578).

4	8	12	16	20	24	28	31
Version	IHL	Type of service		Total Length			
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source Address							
Destination Address							
Options						Padding	

Figure 6. Example Internet Datagram Header (RFC 791:11)

2.6. IPv6

Internet Protocol version 6 (IPv6) is the successor to version 4 Internet Protocol (IPv4) and described as the next generation of Internet Protocol. The main benefits of IPv6 are expanded addressing capabilities, header format simplification, improved support for extensions and options and flow labeling capability (Deering & Hinden 1998). The Figure 7. describes IPv6 header format in detail.

Version	Traffic Class		Flow Label				
Payload Length				Payload Length		Hop Limit	
Source Address (128-bit)							
Destination Address (128-bit)							

Figure 7. IPv6 header format (RFC 2460: 4).

2.7. Wireless Sensor Networks

A wireless sensor network is typically a group of interconnected (Ad Hoc) tiny embedded devices which collectively perform certain tasks. Different protocols have been used for WSNs, such as Zigbee, 6LoWPAN and HART protocol. These protocols share the same PHY/MAC standard IEEE 802.15.4. A typical WSN may consist of up to several hundreds of nodes. Every sensor node has at least a radio transceiver, a microcontroller or a microprocessor, some memory, one or several sensors and a power source. A sensor node is often powered by batteries, but harvesting energy from the environment, such that thermal, light or vibration energy etc. are also being considered. System on chip (SoC) solutions have further aided towards lesser energy consumption (Roundy, Steingart, Fréchette, Wright, Rabaey: 2004).

2.8. Ad Hoc Networking

The term “ad hoc network” is typically applied to a set of wireless nodes that are deployed within the communication range of other nodes, and become a part of a network only during the communication session. The links are usually temporary, because the nodes may leave or new nodes may enter to the network at any time. It might be so that there is no fixed infrastructure at all. In that case all the networking operations must be performed in a distributed manner. If new nodes enter or leave the network, the routing table is updated accordingly (Boukerche: 2006).

There are certain advantages of ad-hoc networking. For example there is no necessary need for separate base stations. The network can be deployed on fly, and it automatically initializes itself. Moreover the network is easily reconfigurable and quickly adapt to any change in topology. Ad-hoc networks are robust against single device malfunctioning since the breakage of any single node does not necessarily affect overall networking performance.

There are certain research challenges involved with ad hock networking, such as the distributed nature of operation poses a control difficulty. Revision of traditional distributed algorithms is necessary before any actual application (Boukerche: 2006). The maintenance of the networked devices can also be expensive e.g. change of batteries etc.

2.9. IEEE 802.15.4

IEEE 802.15.4 standard specifies the physical (PHY) and medium access control (MAC) layers for low power Wireless Personal Area Networks (WPAN). Upper layers are left open for the user to implement custom solutions as presented in Figure 8.

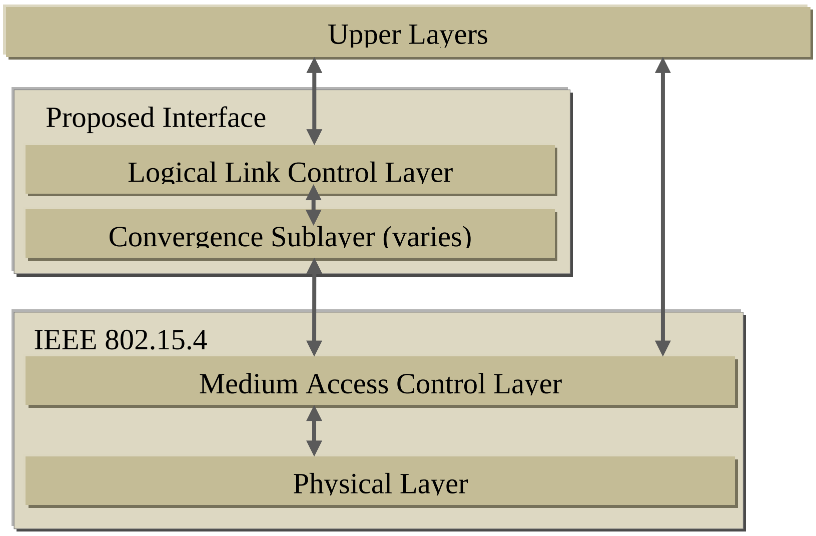

Figure 8. Low-Rate WPAN device architecture.

IEEE 802.15.4 supports three PHY modes. These modes are 868 MHz with data rate of 20 kbps, 915 MHz with data rate of 40 kbps and 2.4 GHz mode with 250 kbps data rate. It implements Carrier Sense Multiple Access algorithm with collision avoidance (CSMA-CA) and it can support up to 64k nodes with 16-bit addresses.

IEEE 802.15.4 supports both peer-to-peer and star networks topologies. Every network must have at least one full function device (FFD) as the network coordinator. Each node has its own unique 64-bit or 16-bit identification address depending on circumstances. The reduced function devices (RFD) are usually implemented using minimum recourses and capacities (IEEE Std. 802.15.4 2003:13—14).

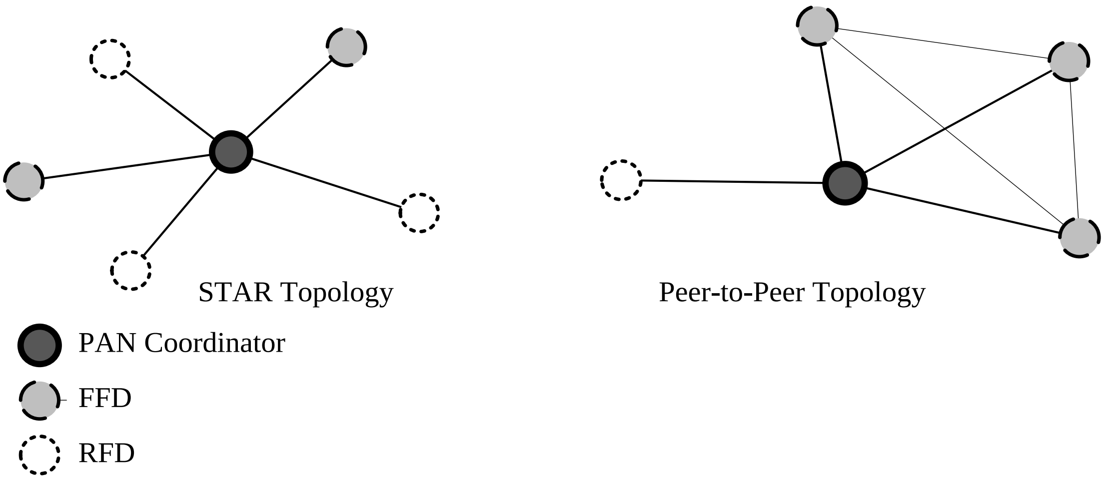

Figure 9. IEEE 802.15.4. Supported Network Topologies.

2.10. 6LoWPAN

The abbreviation 6LoWPAN comes from IPv6 over low power wireless personal area network. It is also a name of an IETF working group. Its features as mentioned by Shelby (2009) include support for 64-bit and 16-bit IEEE 802.15.4 addressing, usefulness with low power link layers, efficient header compression and network auto configuration using neighbor discovery services.

6LoWPAN supports unicast, multicast and broadcast type of transmissions. Fragmentation support allows conversion of 1280 byte IPv6 MTU to 127 byte of IEEE 802.15.4 frames. It supports the use of link layer mesh and IP routing. (Montenegro, Kushalnagar, Hui & Culler 2007; Shelby 2009). The 6LoWPAN protocol stack is described in Figure 10.

Application		ApplicationLayer
UDP	ICMP	Transport Layer
IPv6 with LoWPAN		Network Layer
IEEE 802.15.4 MAC		Data Link Layer
IEEE 802.15.4 MAC		Physical Layer

Figure 10. 6LoWPAN Protocol Stack.

The 6LoWPAN group has defined mechanisms to encapsulate and compress the header up to 4 bytes (Mulligan 2007) as illustrated in Figure 11. UDP compressed header provides the same information as the normal UDP header. These mechanisms make IPv6 based communication possible, for small devices, over IEEE 802.15.4 network (Shelby 2009).

← IEEE 802.15.4 Frame (127 Bite) 64 Bit Addressing →					
21B	1B	40B	8B	53B	4B
MAC	L	IPv6	UDP	Payload	FCS

← IEEE 802.15.4 Frame (127 Bite) 16 Bit Addressing →				
9B	2B	4B	108B	4B
MAC	L	UDP	Payload	FCS

Figure 11. Full UDP/IPv6 (64-bit addressing) and Minimal UDP/6LoWPAN (16-bit addressing).

Compression of TCP header is not included to the RFC4944. The reason is that connection oriented protocol such as TCP generate too much overhead traffic to establish active connection.

2.11. Communication Security

In a wireless network, it is important to secure the data transmissions to avoid unauthorized devices or users. For example, in military applications it is necessary to ensure that the network does not leak information to unknown neighbors. Data security functions can be implemented at any of the different layers, like at the application layer by using advanced encryption standard (AES) or data encryption standard (DES). Security can also be implemented at transport or network layers like TLS or socket secure layer (SSL) or IPSec. In context of WSNs we need security algorithms which are light-weight in terms of computation and communication. Different security loopholes in WSNs and encryption algorithms such as SPINS, TinySec, μTESLA etc. have been investigated (Saraogi 2005; Xiao, Walters, Liang, Shi, Chaudhary 2007: 367-410). A mutual authentication protocol (AMULET), and Secret Search Protocol (SSP) have been discussed in context of RFID applications (Huang & Shieh 2010).

3. RADIO PATH PROPERTIES

3.1. Noise

Noise is a common name to all external electromagnetic disturbances of the transmitted signal. Typical sources of noise are thermal and atmospheric radiation. Also signals transmitted by other devices can be considered as noise in one particular transmissions point of view. The noise is usually modeled as additive white Gaussian noise (AWGN). To measure the quality of a signal with respect to noise, a metric Signal to Noise Ratio (SNR) is employed. It describes the strength of the signal relative to the background noise. Mathematically it is defined as a ratio between signal and noise power levels.

$$SNR = \frac{P(signal)}{P(noise)} = \left(\frac{A(signal)}{A(noise)}\right)^2 \qquad (3.1)$$

Where A is the root mean square (rms) value of signal and noise amplitude.
SNR is more often measured in decibel (dB) scale

$$SNR(dB) = 10\log_{10}\frac{P(signal)}{P(noise)} = P(signal, dB) - P(noise, dB) \qquad (3.2)$$

3.2. Fading

Fading is the attenuation experienced by the transmitted signal while it travels through a propagation medium. Fading varies with respect to certain parameters like time, frequency of the signal, and geographical location. Because of that, the fading is usually modeled as a random process.

3.2.1 Multipath Fading

Multipath fading is caused by the interference of the received signal, which has propagated via different paths but arrived almost at the same time. This type of fading is mostly seen when there are large obstacles such as buildings, walls, cliffs or atmospheric differences. in the area of transmission. The multipath can cause either constructive or destructive interference or phase shift of the signal. Suppose that the transmit power at time 0 is given by

$$x(t) = \delta(t). \quad (3.3)$$

Then the received multipath attenuated signal power is given by

$$y(t) = \sum_{n=0}^{N-1} \alpha_n(t) e^{j\theta_n} \delta(t - \tau_n), \quad (3.4)$$

where N is equal to received multipath signals, $\alpha_n(t)$ is the attenuation factor, τ_n is the time delay of n_{th} signal and $e^{j\theta_n}$ is the phase of the received signal (Proakis & Salehi 2008: 831-833).

3.2.2 Shadow Fading

If the mobile receiver is situated behind a large obstacle and it experiences a significant loss in received signal power. This phenomenon is called shadow fading.

3.2.3 Slow Fading and Fast Fading

Slow and fast fading are related to the Doppler spread of the channel and they are usually associated to mobile devices. Slow fading occurs if the coherence time of the channel is larger than the symbol period of transmitted signal. This situation can be caused by shadowing effect. The amplitude and phase change can be considered as constant during the transmission time period. The average power distribution is nearly Gaussian for small areas at almost same distance from base station.

Fast fading occurs when the coherence time of the channel is small compared to the symbol period of the transmitted signal. Fast fading is usually caused by interference of locally reflected signal paths. A sliding window averaging technique can be used to separate slow fading and fast fading from each other (Bertoni 1999; Haykin, Moher 2005).

3.2.4 Flat Fading and Frequency Selective Fading

Flat fading results if the bandwidth of the transmitted signal is smaller than the coherence bandwidth of the channel. The Signal-to-Noise ratio decreases in flat fading channel. Such channels are also known as narrowband channels (Rappaport 2007:205-209).

If certain frequency components of the signal attenuate more than others, the phenomenon is called frequency selective fading. This kind of fading normally occurs when the bandwidth of transmitted signal is greater than coherence bandwidth of the channel. These sorts of channels are also known as wide-band channels. Figure 12 illustrates the fading experienced by the signal as a function of baseband signal bandwidth (Bertoni 2000; Haykin, Moher 2005; Belloni 2004).

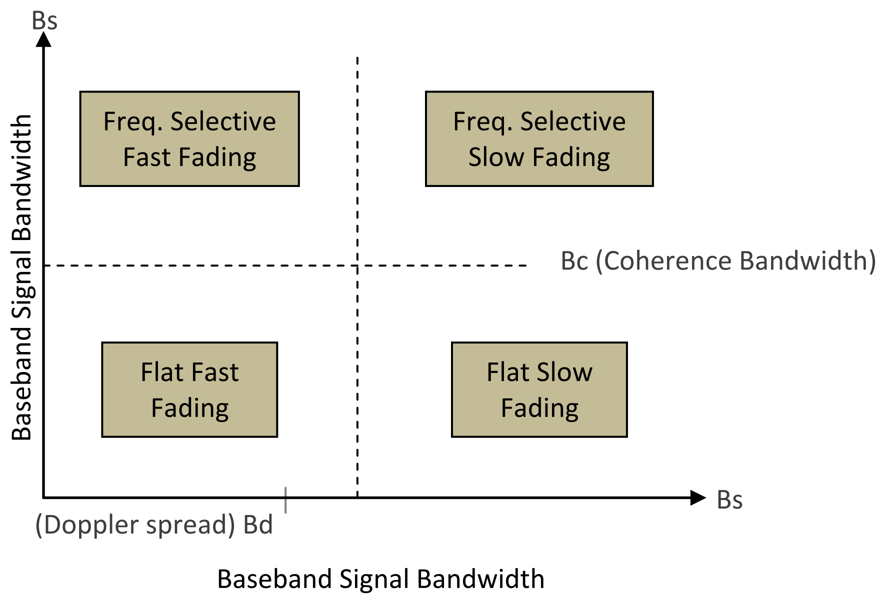

Figure 12. A quadfield presentation of the types of fading experienced by the signal as a function of baseband signal bandwidth.

3.2.5 Deep Fading

Deep fading appears as a result of strong destructive interference between multipath components of a signal. As a result the signal to noise ratio (SNR) of the channel drops severely and sometimes the communication may break temporarily.

3.3. Commonly Used Fading Models

3.3.1 Nakagami Fading

Nakagami distribution is used to model the fading in a wireless channel due to multipath effect where the delay time-spread is relatively large. (Linnartz 2009). Its empirical development was based on measurements. Mathematical representation of Nakagami probability density function (pdf) is:

$$f(r) = \frac{2}{\Gamma(k)}\left(\frac{k}{2\sigma^2}\right)^k r^{2k-1}\, e^{-\frac{kr^2}{2\sigma^2}} \qquad \text{and} \quad r \geq 0, \tag{3.5}$$

where $2\sigma^2 = E\{r^2\} = \Omega$ is the second moment and $\Gamma(\mathrm{k})$ is the Gamma function which is defined as

$$\Gamma(\mathrm{k}) = \int_0^\infty t^{k-1} e^t \, dt. \tag{3.6}$$

The fading figure k is defined to be greater than or equal to 0.5 and it is calculated as a ratio of moments. The amplitude of equivalent base band signal is represented by r. If we set the value k equal to one, the Nakagami distribution reduces to Rayleigh distribution (Nakagami 1960; Linnartz 2009).

3.3.2 Weibull Fading

Iassume that X1 and X2 are independent identically distributed (i.i.d) zero-mean Gaussian variables. If we change the Rayleigh distributed random variable $R = (\mathrm{X}_1 + \mathrm{X}_2)^{\frac{1}{2}}$ to $\mathrm{R} = (\mathrm{X}_1 + \mathrm{X}_2)^{\frac{1}{\mathrm{k}}}$ then the corresponding probability density function (pdf) becomes Weibull distributed. Mathematically it can be defined as

$$f(r) = \frac{kr^{k-1}}{2\sigma^2} e^{-\frac{r^k}{2\sigma^2}}, \tag{3.7}$$

where $2\sigma^2 = E\{r^2\} = \Omega$ is the second moment. Weibull fading is an effective model for both outdoor and indoor environments. In (3.7), $k < 1$ indicates infant mortality, $k = 1$ means random failures (independent of age) and $k > 1$ indicates wear out failures (Belloni 2004; Abernethy 2006).

3.3.3 Rayleigh Fading

In the Rayleigh fading model it is assumed that significant line of sight (LoS) communication cannot be applied. This model is typically important in areas which contain a large number of obstacles between the transmitter and the receiver. As a consequence, the signal is well scattered when it reaches the receiver. If X1 and X2 are i.i.d zero-mean Gaussian random variables, the envelop $R = (X_1 + X_2)^{\frac{1}{2}}$ is Rayleigh distributed random variable. The pdf is represented as

$$f(r) = \left(\frac{r}{\sigma^2}\right) e^{-\frac{r^2}{2\sigma^2}} \quad \text{and} \quad r \geq 0, \tag{3.8}$$

where $E(r^2) = 2\sigma^2 = \Omega$ is second moment and r is the amplitude of equivalent base band signal. The fading figure k is equal to one. The phase is independent from the amplitude and uniformly distributed while the power is exponentially distributed (Belloni 2004).

3.3.4 Rician Fading

Rician fading model assumes that the signal is partially cancelled by itself due to multipath interference with a strong LoS signal. If X1 and X2 are non-zero-mean Gaussian random variables, then the envelope $R = (X_1 + X_2)^{\frac{1}{2}}$ is Rician distributed. The Rician pdf is represented as

$$f(r) = \left(\frac{r}{\sigma^2}\right) e^{-\frac{r^2+v^2}{2\sigma^2}} I_o\left(\frac{rv}{\sigma^2}\right) \qquad and \qquad r \geq 0, \tag{3.9}$$

where $v^2 = v_1^2 + v_2^2$ is the power of the signal LoS component and I_o is a modified Bessel function of order zero. $\frac{v^2}{2\sigma^2} = K$ is called the Rician factor. It is the relation between the power of LoS component and the power of Rayleigh component. If $K \to \infty$ it indicates that there is no LoS component and the Rician distribution reduces to Rayleigh distribution (Belloni 2004).

3.3.5 Log-Normal Shadow Fading

Log-Normal shadow fading models the long term variation in the signal strength. If X is normally distributed random variable having a mean μ and variance σ^2, the envelope $R = e^X$ is log-normal distributed random variable. The pdf is given as:

$$f(r) = \begin{cases} \frac{1}{r\sigma\sqrt{2\pi}} e^{-\frac{(\ln(r)-\mu)^2}{2\sigma^2}} & , \quad r > 0 \\ 0 \, , & \quad r \leq 0. \end{cases} \tag{3.9}$$

3.4. Path Loss

Path loss is the attenuation of transmitted signal as a function of distance between transmitter (Tx) and receiver (Rx).model parameters must be selected individually to each particular environment.

3.4.1 Path Loss Exponent

Typically the signal power drops as an exponent of distance between Tx and Rx. For free space the path loss exponent is 2 and

$$L \propto d^2 \qquad or \qquad L = \frac{4\pi f d^2}{c} \, , \tag{3.10}$$

where f is the frequency of the transmitted signal and c is the speed of light in free space.

3.4.2 Model Equation

In general, the loss L in decibel scale can be described as

$$L(dB) = 10\ n\ log_{10}(d) + C, \tag{3.11}$$

where n is the path loss exponent, d is the distance between transmitter and receiver and C is a loss constant (Rappaport 2007).

4. DISTANCE BASED LOCALIZATION

For distance based localization, first the inter node distances are calculated for each or most of the node in the WSN and then algorithms are applied to generate absolute or relative map of the network. Trilateration is one of the basic algorithms used for distance based localization. Yang , Zheng & Yunhao Liu (2008) propose a confidence based iterative localization approach based on quality of trilateration (QoT). Multidimensional Scaling (MDS) is another technique that makes use of matrices and a method known as Singular Value Decomposition (SVD) to construct map of the sensor network. This method has been thoroughly investigated over the years and many improvements have been suggested. Y. Shang and W. Ruml (2004) have presented one such improvement for MDS based localization.

4.1. Challenges

One of the main challenges in distance based localization is poor ranging measurements. Sensor nodes are not equipped with sophisticated ranging equipment to keep the price as low as possible. Therefore achieving accurate range measurements is difficult.

The environment is usually dynamic, especially for outdoor deployments. This affects the transmission of signals between any two sensor nodes and makes received signal strength based distance estimation more difficult. Sensor nodes usually transmit with very little transmission power. These weak signals are easily attenuated by noise and other wireless signals in the area.

Therefore if a sensor node estimates distances to its neighbor nodes based on received signal strength, some of these estimates could be wrong. In this thesis a method of filtering out the faulty estimates is described and its merits are investigated.

4.2. Reference Nodes

A reference node is one which knows its own position in two or three dimensional space. All other nodes calculate their own locations based on their distances to the neighboring reference nodes. If there is no reference node available in the WSN then the localization map is only accurate to local coordinate system. There can be more than one local coordinate systems based on the clusters within the network. Density of reference nodes improves the overall localization of the network.

4.3. Network Localization Approaches

A network can be localized in centralized or distributed manner. In centralized approach all inter node distances are collected at a single node where most of the calculations are performed and a localization map is generated. Then this node may inform each node about its location. This method is good for in such networks where the nodes need to be localized only once or very rarely after their deployment. The reason is that this method introduces a lot of transmission overhead. This method can be useful if the nodes remain static for long periods of time and their normal mutual communication is used for collecting RSSI data.

In distributed approach the network is realized as collection of smaller clusters. The global map is constructed by combining the smaller local maps. For example: David Moore, John Leonard, Daniela Rus and Seth Teller (2004) have described a distributed network localization algorithm based on robust quadrilaterals.

4.4. RSSI Based Distance Estimation

For a WSN consisting of small and inexpensive sensor nodes, RSSI based localization is usually the only available option. RSSI has been extensively reviewed in literature as a basis of distance estimation between wireless nodes. Many variations and improvements have been suggested so far. Srinivasan & Levis (2006) discuss that RSSI is a good indicator of link quality for newer radios such as CC2420, while it is measured above sensitivity threshold. Tian, Shuang, Xinming Zhang, Pengxi Liu, Peng Sun, Xinguo Wang Li, Xiaoli, Hongchi Shi & Yi Shang (2007) propose an RSSI based DV-hop algorithm to reduce estimation error. Li, Shi and Shang (2005) proposed sensor network localization algorithm based on sorted RSSI quantization scheme. Zang, Liang and Yu (2007) proposed a probabilistic analysis of RSSI based distance estimation. Lau, Lee, Lee and Chung (2008) proposed an enhanced RSSI based high accuracy real time user location tracking system.

To achieve an accurate distance estimate, the measured RSSI must also be accurate. Algorithms that can improve the measured RSSI are very useful. Pu and Chung (2008) propose an algorithm to improve RSSI by eliminating noise caused by multipath fading. Algorithms like SVD Reconstruct (Drineas, Javed, Magdon-Ismail, Pandurangan, Virrankoski & Savvides 2006) are especially useful for reconstructing Euclidian distance matrix when only partial distance information is available.

5. SYSTEM DESCRIPTION

A node to node connection was made to collect sufficient data for further research. First the description and specification of the used hardware is given and then the description of developed system is explained in detail.

5.1. Hardware

We used the Sensinode Nano Series nodes for the experimental data collection and testing. Following is a brief description of the Sensinode applied hardware.

5.1.1 Sensinode Nano Series Platform

The Sensinode Nano Series evaluation kit contains a development board (DevBoard D210), an usb router (N601), two sensor nodes (N711) and a radio modules (N100).

Figure 13. Sensinode Nano Series evaluation kit.

Sensinode Nano Series modules use the radio module RC2301AT from Radiocraft. It has an integrated quarter wave ceramic resonant antenna, built-in location engine and 128 kB flash memory. The IEEE 802.15.4 network implementation is done by using CC2431 system on chip (SoC) RF transceiver solution by Texas Instruments (TI). It contains a modified version of 8051 Single-cycle MCU with 128 kB of flash memory, 8 kB of SRAM and 4 kB EEPROM. It supports 19 digital and analogue I/Os, 8 channel 14 bit ADC, UART, SPI and debug interfaces. It has a 32.768 kHz real time clock (RTC) crystal and 4 timers. The RF transceiver uses direct sequence spread spectrum (DSSS) and 16 channels in the 2.45 GHz ISM band with 2 MC/s chip rate, giving a raw data rate of 250 kb/s. The signal is modulated by using Offset–Quadrature Phase Shift Keying (O-QPSK). The DSSS provides a robust performance in noisy environments where other applications may use the same frequency band as well (Radiocrafts AS 2007; Sensinode Ltd 2007).

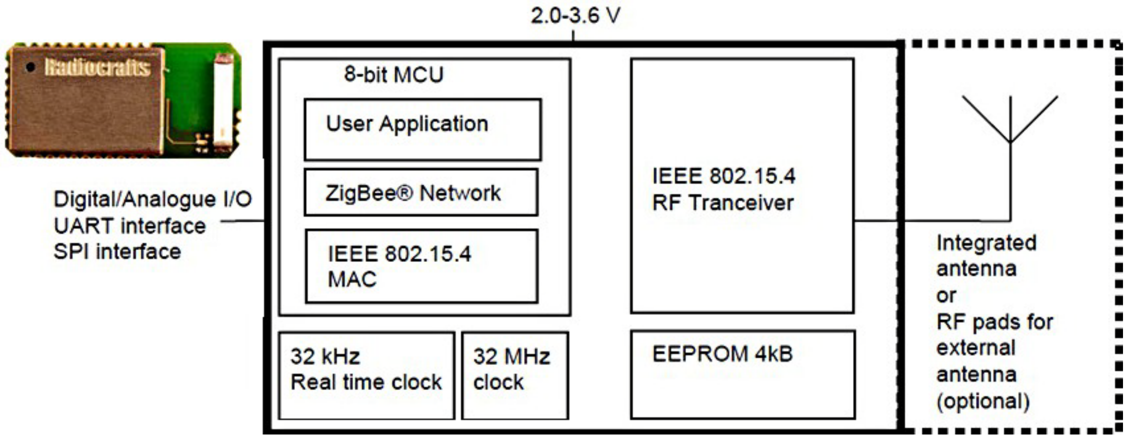

Figure 14. A picture and schematics of Radiocraft RF module N711.RC2301.

5.2. Developed System Description

5.2.1 Gateway Node

The NanoRouter N601 is used as a gateway node. It is programmed to operate as a full function device (FFD) in our experiments. This device has the same radio characteristics as explained in section 5.1.1. The gateway node is connected to a personal computer (PC) by universal serial bus (USB) interface (FTDI232B). It enables a direct control of the gateway node. To program the node we have to use DevBoard D210 with UART/SPI connection. The NanoRouter N601 also has two LEDs to aid the tracking of ongoing process and debugging.

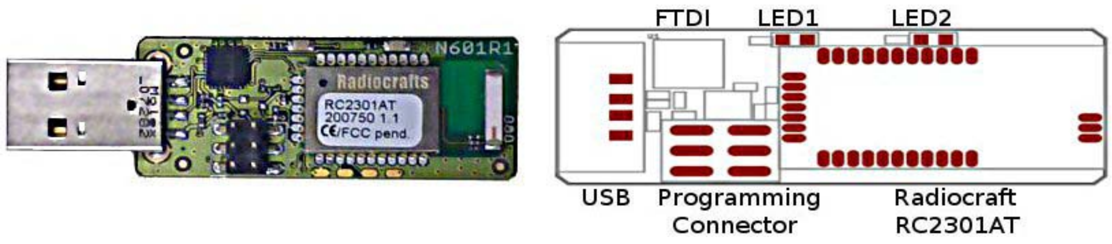

Figure 15. A picture and schematics of Sensinode NanoRouter N601.

When the router node receives a command from PC application, it broadcasts a specific signal associated to that command to neighbor nodes. Detailed explanation of the process is given in next chapter.

5.2.2 Sensor Node

The NanoSensor N711 is programmed to be a reduced function device (RFD) for the experiments in context of this thesis. This device is powered by two AA size batteries. The node has a temperature sensor and a light sensor for environment monitoring but these measurements were not used in our experiments.

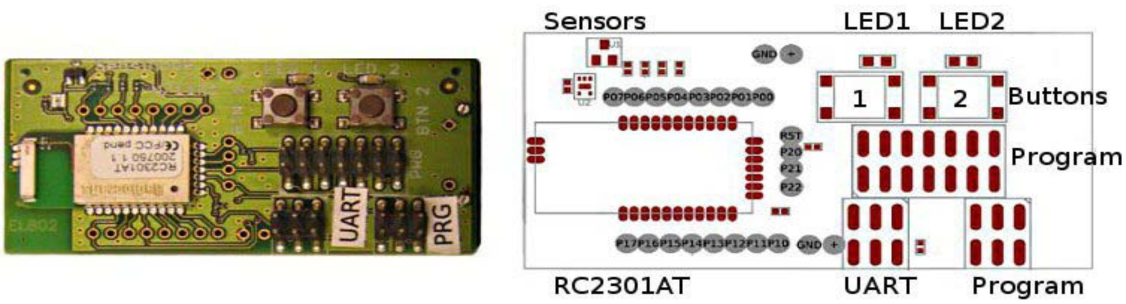

Figure 16. A picture and schematics of Sensinode NanoSensor N711.

In our experiments the RFD node was placed in different distances from FFD node to measure the equation of the received signal strength as a function of distance. The distance was set to one meter for the first measurement and then increased by one meter in time. The RFD node stays in idle mode and periodically checks the channel for incoming connection requests. If it receives a certain command from the FFD node, it carries out the action accordingly. A detailed description of the experiments is given in the next chapter.

6. SOFTWARE ARCHITECTURE

6.1. Sensinode NanoStack

Sensinode NanoStack is a 6LoWPAN protocol stack built over IEEE 802.15.4 communication protocol. The stack is implemented with a real time operating system (RTOS) known as FreeRTOS (The FreeRTOS Project). Programs can be developed by using any C-language development tools (windows or Linux). The use of universal Socket Application Interface (API) makes 6LoWPAN application development far easier. The older version of Sensinode NanoStack (v1.1.0) is kept open source. therefore it is possible to make extensions and additions to that older version of NanoStack.

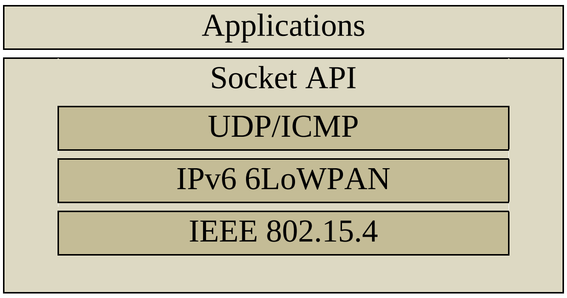

Figure 17. NanoStack Protocol Stack.

6.2. Contiki Operating System

Contiki is developed by a group lead by Adam Dunkels in the Swedish Institute of Computer Science (SICS) (Contiki 2010). The Contiki operating system is kept open source and it supports many different platforms. One kry idea is that Contiki would support both wired and wireless embedded systems and provide an interaction between them. Therefore the support community is far bigger than that of NanoStack. The operating system (OS) is designed to support multi threading operations with very little processing overhead and is ideal choice for microcontrollers with little memory. The

Contiki radio driver for Sensinode devices was not fully functional by the time we undertook our experiments therefore we only used NanoStack based FreeRTOS system to program the devices.

6.3. FFD Node

As described in chapter 5 section 5.2.1, the Sensinode NanoRouter N601 is used as a gateway or FFD node in our experiments. The application program is written in C programming language using NanoStack API which closely follows the Portable Operating System Interface for Unix (POSIX) API (NanoStack 2007). The main task of gateway node was to request simple packets from the RFD at predefined intervals, measure the received signal strength of each received packet, keep track of lost packets, ensure at least 50 successful transmissions and then transfer the data to the PC application. The operation trigger was controlled through the PC application. A flow chart of the gateway node operation is illustrated in Figure 18.

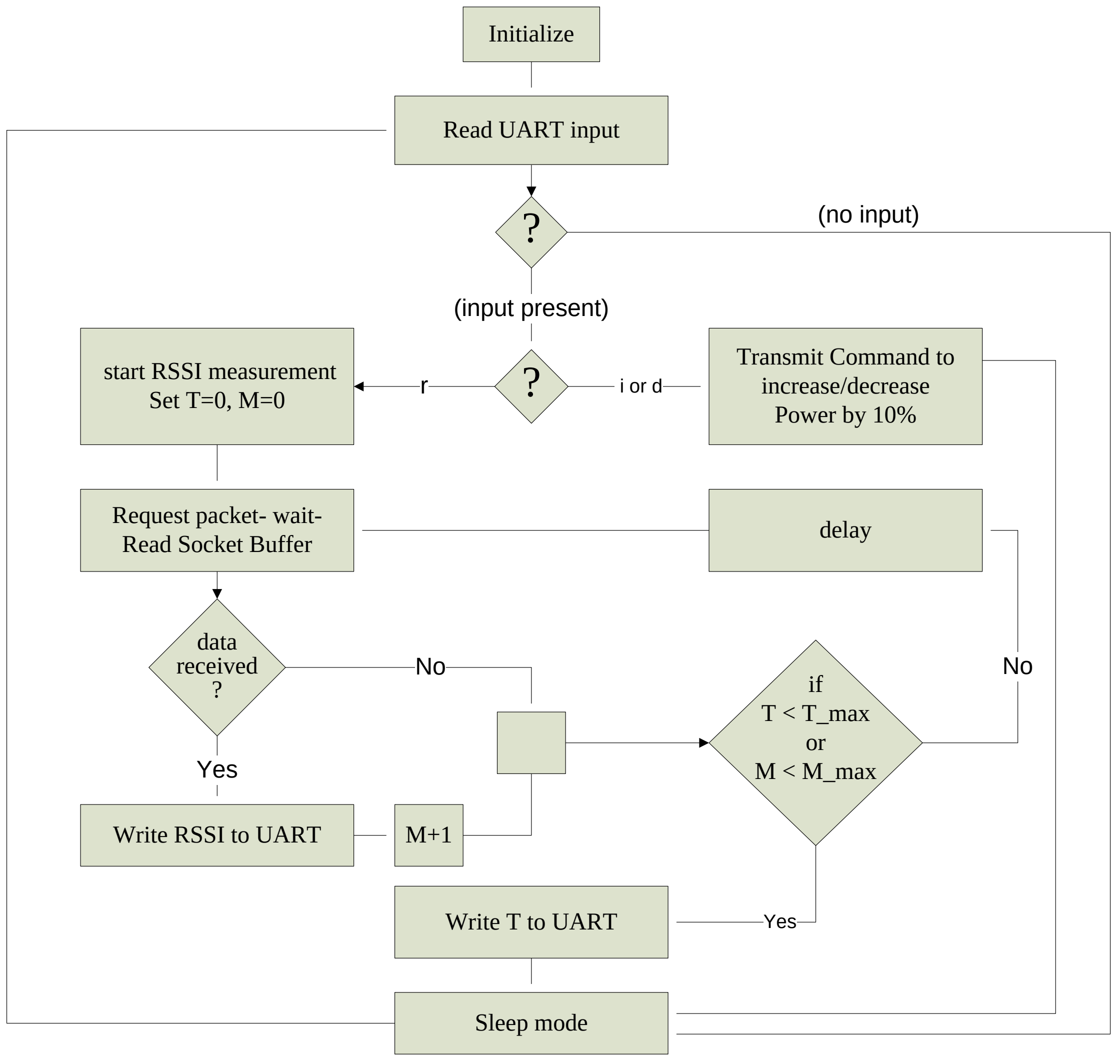

Figure 18. A flow chart of the FFD node operation. T is the number of tries and M is the number of measurements performed.

6.4. RFD Node

The program for the RFD is written in C programming language with NanoStack support. The device sleeps most of the time to save power and checks the channel for any awaiting connection requests from the router. Basic functionality of the RFD is explained in Figure 19.

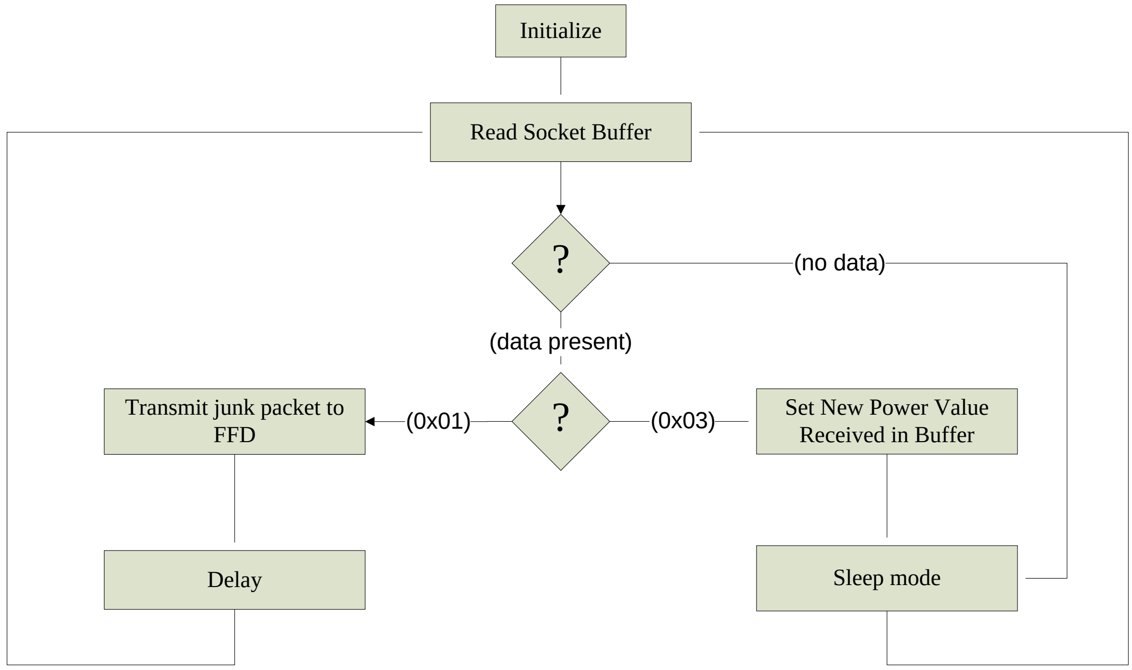

Figure 19. Flow chart of RFD node operation.

6.5. PC Application

The PC application is basically a command line tool which prints the following five commands on PC screen.

- Increase power
- Decrease power
- Start measurement
- Chose file
- Quit

The user is asked to enter the number of the required command. When the user enters the number, a specific code is transmitted to the FFD by using USB interface. The FFD carries out the operation related to that code.

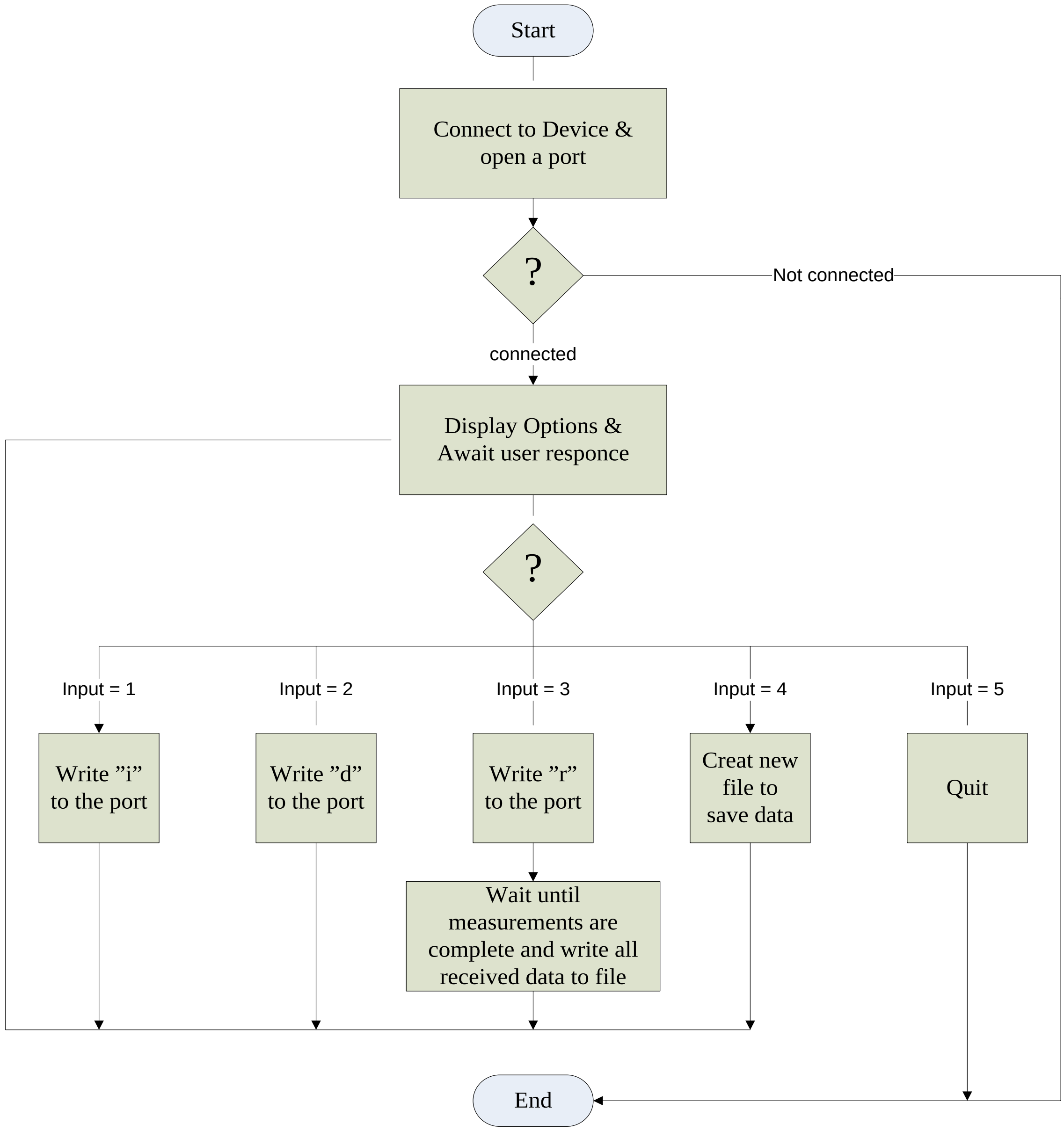

Figure 20. A flow chart of the PC application.

6.6. A Structure of the Collected Data

The collected data is saved as text file. Each distance has its own row and each row contains 50 received signal strength (RSS) measurements in decibel milliwatt (dBm) at that particular distance. An RSS measurement is the power dBm calculated by adding the

RSSI register value and the RSSI offset value (CC2430 2009: 168). The last value in every row is the number of tries needed to achieve 50 successful transmissions. The distance between FFD and RFD was increased in a step of one meter. As a consequence the number of each row indicates the distance in meter between FFD and RFD. The text files were saved with appropriate name for each experiment with txt extension. The data is space separated integer values. These data files are directly readable to the analysis application developed in Matlab as an N x M matrix where N is the number of rows and M is the number of columns.

7. EXPERIMENTAL SET UP

The experiments conducted in the context of this thesis are divided into two parts, indoor and outdoor experiments. The location for the experiments was around the premises of the University of Vaasa.

7.1. Outdoor Measurements

Outdoor measurements were taken in the parking area between Fabriikki and Technobothnia buildings at the University of Vaasa. Line of sight connection was ensured but the multipath effect was expected to be present as well.

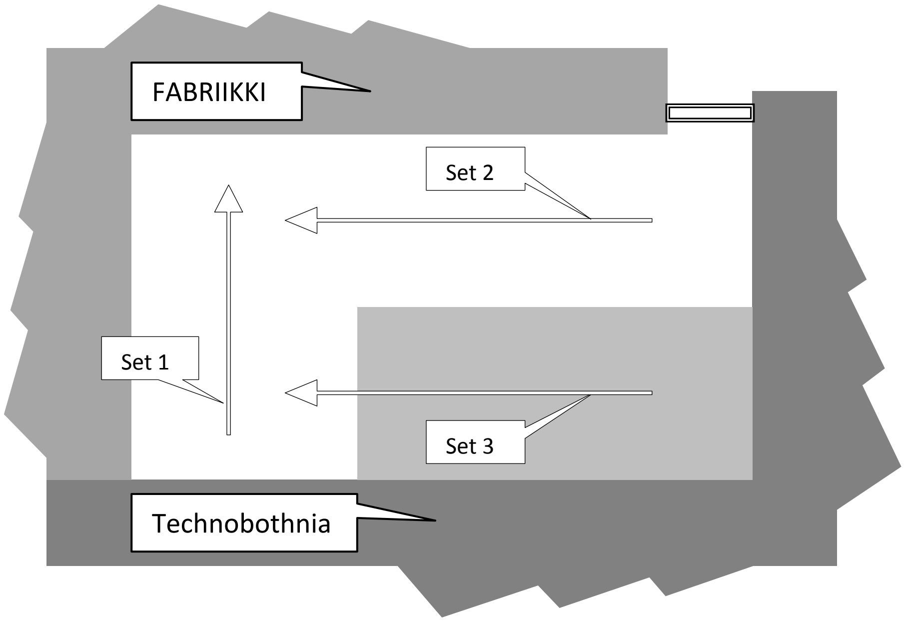

Figure 21. Location of outdoor experiments.

Each set of experiments was started with 1 meter distance between the FFD and RFD nodes. The FFD node was kept stationary while the RFD node was moved further apart in

1 meter steps, 50 RSS measurements were collected from each distance. The distance was increased until the FFD and RFD fail to establish a communication link. The maximum limit of distance for reliable communication found in our experiments, using the built-in ceramic antenna, was 30—35 meter.

7.2. Indoor Measurements

Indoor experiments were conducted in the corridors of Technobothnia building. The surroundings consist of concrete walls and columns, wood and steel structures and electronics equipment. Wireless local area network (WLAN) 802.11 signal was also strong inside the building. Therefore this setup provides a perfect test bed environment of any modern facility where 802.15.4 sensor network is required to be installed such that they operate simultaneously with WLAN. The measurements were collected in the same way as in the outdoor experiments to achieve a reasonable comparison between these two environments.

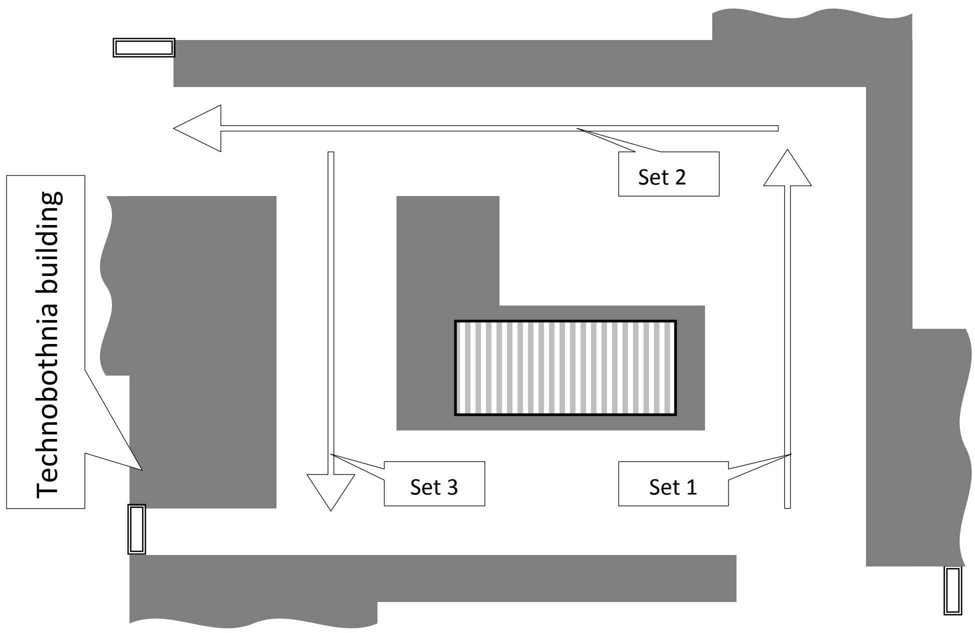

Figure 22. Location of indoor experiments.

8. ANALYSIS AND RESULTS

The data was analyzed using MATLAB. A graphical user interface (GUI) was developed to easily visualize and optimize the model parameters.

8.1. Preprocessor

The GUI allows the user to load the data file obtained from one of the experiments. The preprocessor automatically reads the file and prepares the information present in the file for further analysis. Let's assume that the data is presented as N x M matrix of integer values. As described in chapter 6 section 6.6, the number of rows N determines the maximum distance between FFD and RFD to which the experiments have been conducted. This information is collected by preprocessor and displayed in the GUI as End Distance = N meter. The starting distance is set to 1 meter but the user can chose to analyze measurements at any starting and ending distances if desired.

The last column consists of the number of tries needed to obtain 50 successful measurements. This number is always greater than or equal to 50. The preprocessor subtracts 50 from these numbers to find the number of lost packets. The minimum and maximum number of lost packets is displayed on the GUI.

The matrix N x M-1 contains the received signal power values computed by adding the RSSI register value and the RSSI offset value (CC2430 2009: 168). The preprocessor reads each row and calculated the standard deviation (SD) of RSS. This information is saved for further analysis. Also the maximum and minimum values are displayed on the GUI. The preprocessor also calculated the mean value for each row and saves it for further analysis.

8.2. Model Equation

Chipcon specifies the following formula for CC2431 to relate RSSI in dBm to the distance between transmitter and receiver (Aamodt 2006).

$$RSSI = -10\ n\ log_{10}(d) + A, \tag{8.1}$$

where n is the propagation exponent, d is the distance between transmitter and receiver and A is a constant. We have used the same equation for our model

$$d = 10^{\frac{RSSI-A}{-10n}}. \tag{8.2}$$

8.3. Optimization Parameters

There are four parameters to be optimized.

- Limit of SD of RSS
- Limit of Number of Lost Packets
- Propagation Exponent
- Constant of Model Equation

The limit of SD of RSS serves as a filter to eliminate all those mean values of RSS that are outside the optimized SD limit. These discarded measurements are replaced by NA and thus do not affect the outcome of cost function.

Similarly the limit of number of lost packets also serves as a filter to discard all those mean values of RSS that fall outside this limit.

Propagation exponent n and the constant A are the parameters for the fitting curve.

8.4. Cost Function

The cost function (CF) calculates the absolute value of the difference between the original distances and the estimated distances. The original distance vector d is generated automatically starting at one meter and ending at N meter with one meter intervals. The estimated distance vector d* is generated by using model equation and optimized model parameters.

$$\mathrm{CF} = |\, \mathrm{d} - \mathrm{d}^{*}|. \tag{8.3}$$

8.5. Parameter Optimizer

The parameter optimizer is basically a bounded fminsearch operation (Errico 2006) which optimizes four parameters of the model. The fminsearch operation requires an initial guess for these four parameters in order to perform the optimization. It is possible that multiple local optimal solutions exist for a certain case. By choosing suitable initial guesses for the parameters near global optimal solution can be found.

The bounded fminsearch operation takes into account the maximum and minimum possible values of the parameters and does not exceed those limits during the optimization process.

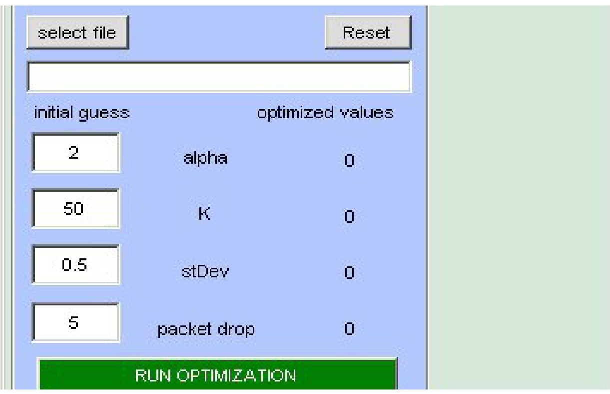

Figure 23. The first part of data analysis GUI (auto optimization of model parameters).

When the optimization process is complete an auto script plots the mean values of RSS along with the fitted curve in figure one. And in the second figure a comparison between original distance and the estimated distances is plotted for visual inspection. The operation is illustrated in Figure 24.

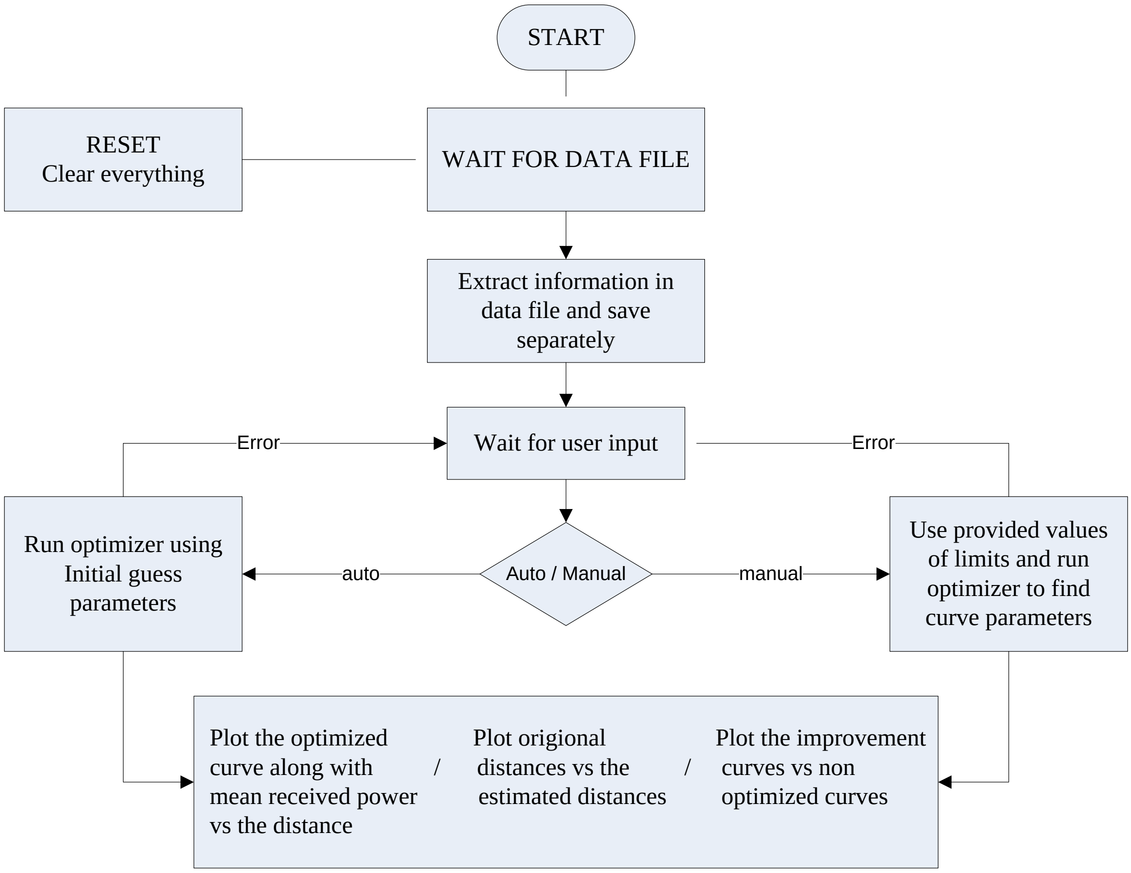

Figure 24. Flow diagram of GUI operation.

The second part as illustrated in Figure 25 lets us select the limits manually. A script updates the graphs and results every time a limit value is changed. In this part we can select custom values for the SD, Packet Loss and RSS threshold. we can also select a different starting and stopping distance on the curve. This is helpful for partial inspection of data. Points which do not fulfill these limits are left out of the optimization process. The RSS threshold was set to -85 dBm but it can be changed within certain range.

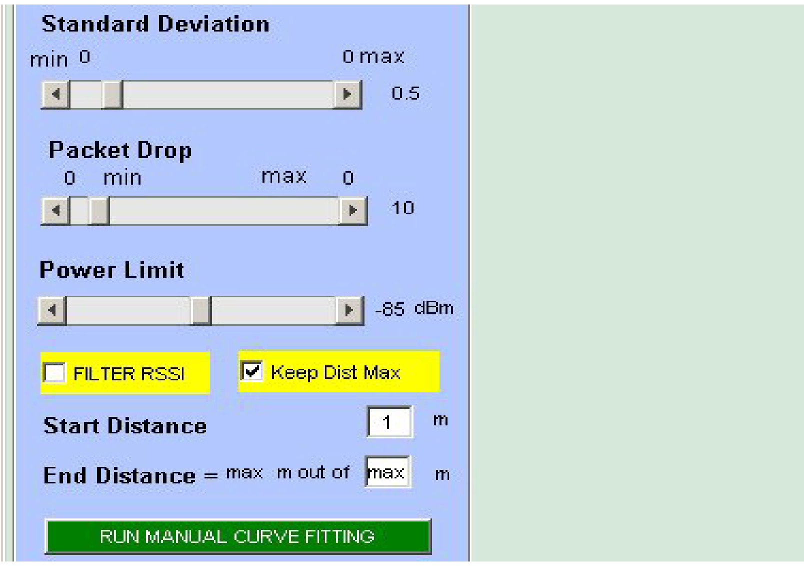

Figure 25. Manual settings of model parameters.

A simple three point moving average filter smoothes out any sharp peaks in the measured RSS data for a certain distance. These peaks are the result of random errors. They can cause major shift in mean value of RSS from the true mean value if left unnoticed. By using the smoothing filter these errors can be corrected to a certain extent.

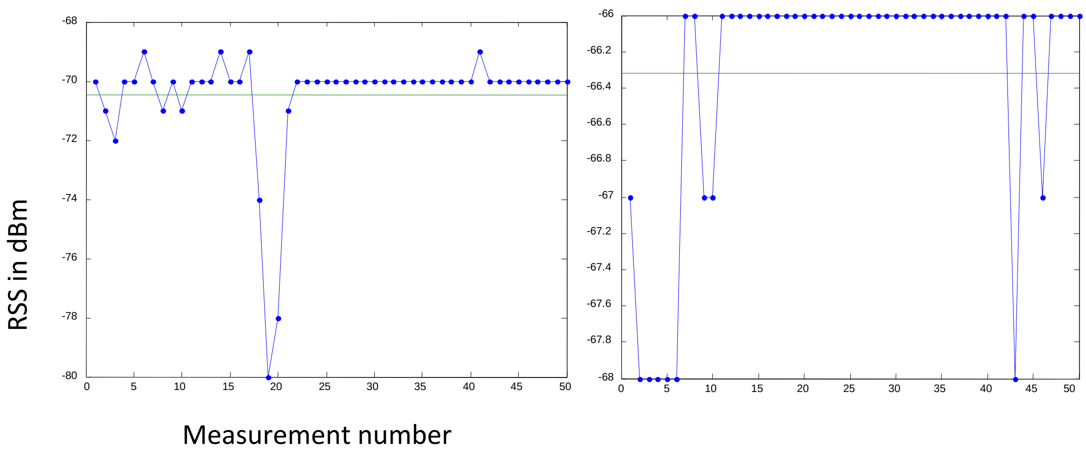

Figure 26. Spikes present in the measured RSS data in dBm.

The last part shows the estimated model curve parameters along with the average distance error calculated using the current model parameters.

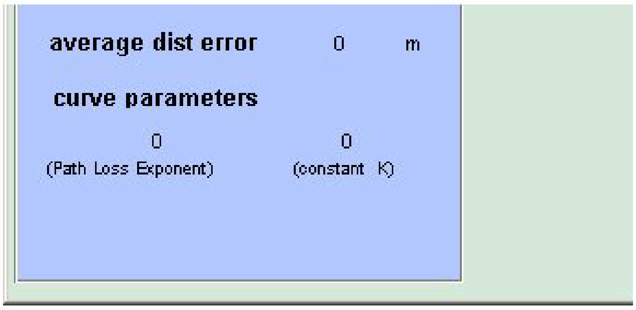

Figure 27. Average distance error and curve parameters.

8.6. Observation

If we examine the measured RSSI data in more detail it appears that for certain distances there are few strong components of RSSI which appear more often during the 50 measurements duration. This results in small SD for that particular measurement. While in other cases the RSSI values are spread over wide range with no strong component.
This results in larger value of SD for that particular measurement. In Figure 27 each block shows the weight of each RSS component for 50 measurements at 1—28 meter distances along the rows one meter increment in distance starting at top row left column.

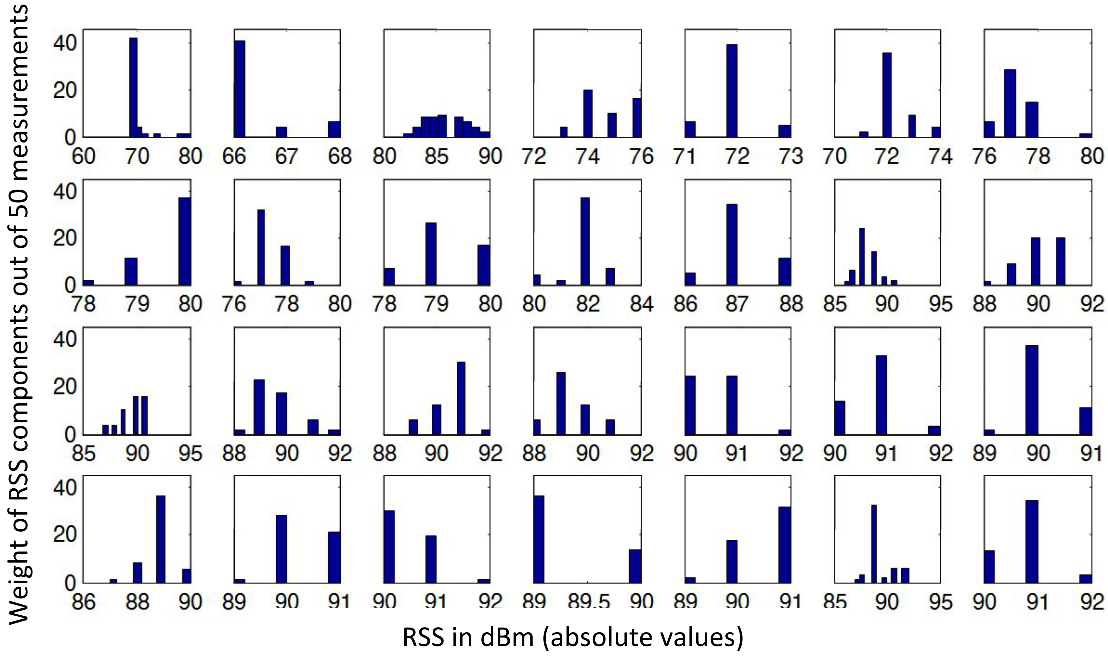

Figure 28. weight plot of RSS in dBm for 1—28 meter distance .

We discuss the effect of SD of RSS on the estimated error in distance in next section. The packet loss rate is direct indication of faulty link. If packet loss rate is recorded to be more than usual, that may also indicate unreliability of that particular link for distance estimation and localization process. In next sections we describe this effect in detail.

8.7. Results and Comparisons

The RSS data collected at the FFD node does not contain any distance information within it. We need an RSS to distance mapping to estimate the approximate distance of the node from which a particular measurement was collected. Figure 29 presents the un-mapped RSS data which is seen by the FFD for 1—28 meter distance and for 50 measurements at each distance. Some components of RSS appear more often. Before any mapping the FFD cannot distinguish between any two components on the basis of distance from which it came.

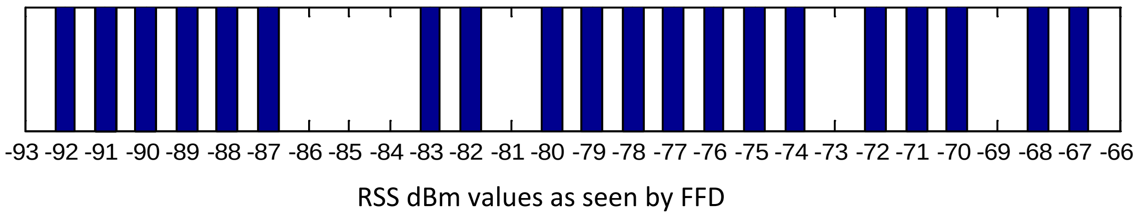

Figure 29. RSS values collected by FFD for 1—28 meter distance before mapping to distance.

The mapping is performed using certain fitting curve parameters, which have been previously estimated using the parameter optimizer. Figure 30 shows a sample data from one of the experiments. The RSS to distance mapping is done using log distance path loss model. It is noticeable that nodes at distance 14 to 28 are all claiming to be at approximate distance of 16—20 meter from the FFD. Obviously some of these distance estimates are true and some are false. The average distance error in this case is high.

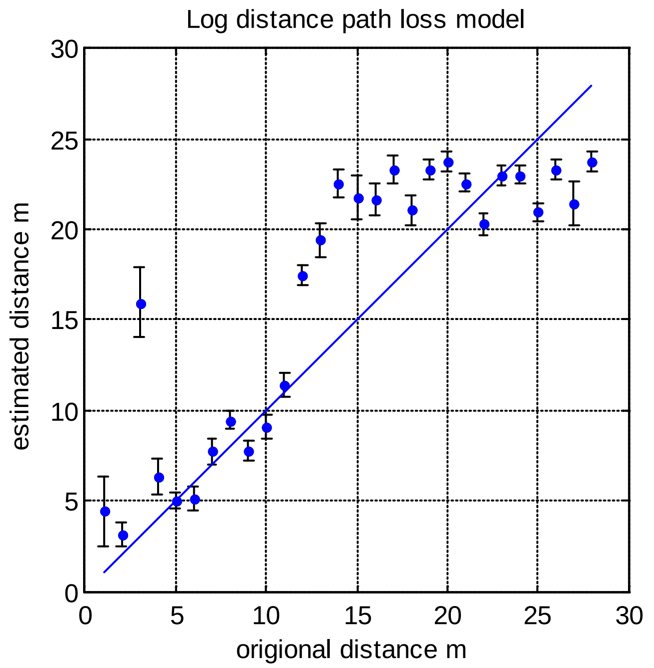

Figure 30. Distance estimates before applying optimized SD and packet loss limits.

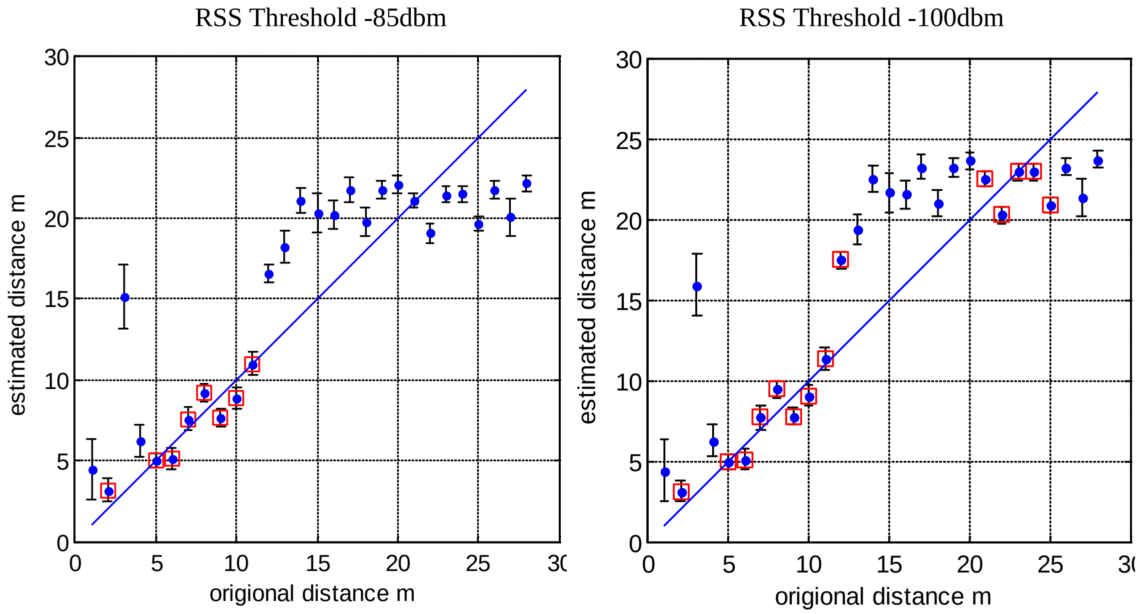

Figure 31. Distance estimates using optimized parameters and limits.

In figure 31 dots in squares represent nodes found within certain error limits while dots without squares represent rejected nodes. The rejection is based on either the RSS threshold or the use of optimized SD and packet loss limits. It can be noticed that by applying these optimized limits, the faulty measurements can be separated from the relatively accurate measurements.

8.8. Analysis

In Figure 31 the average distance error and the number of detected nodes are plotted for a certain set of measurements with respect to SD limit for RSS and packet loss limits. In Figure 31(b) We can notice valleys in the surface plot indicating that certain values of SD and packet loss limits help improving average distance error. While figure 31(a) indicates the number of nodes that fall under certain error limits. for example the three indicated data-points (black dots top to bottom) represent that 10 nodes fall into the error limits of 1.228 meter, 9 nodes fall into the error limits of 0.978 meter and 7 nodes fall into the error limits of 0.743 meter.

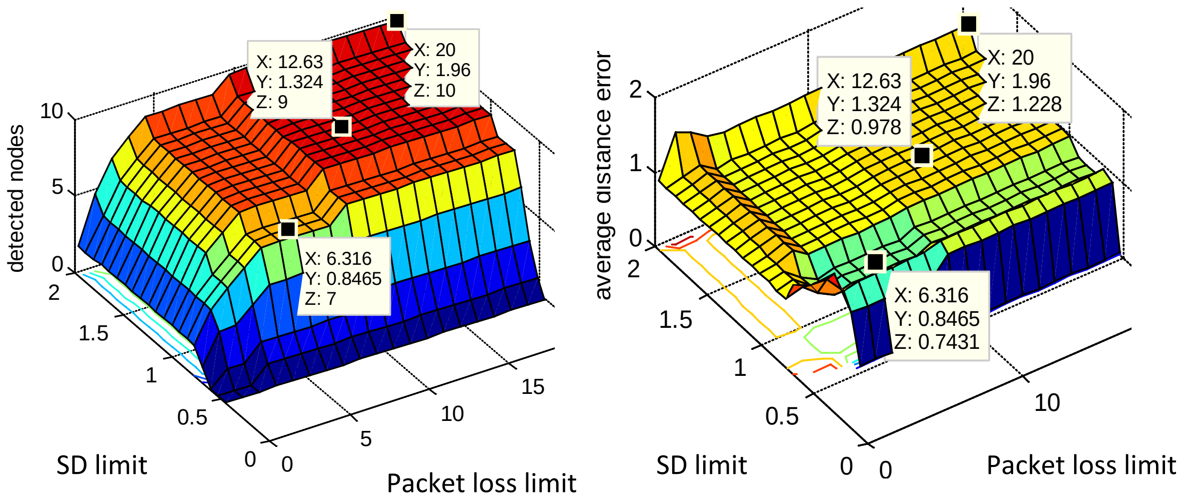

Figure 31. Sample, variation in number of node (left) and average distance error (right) with SD and packet loss limits.

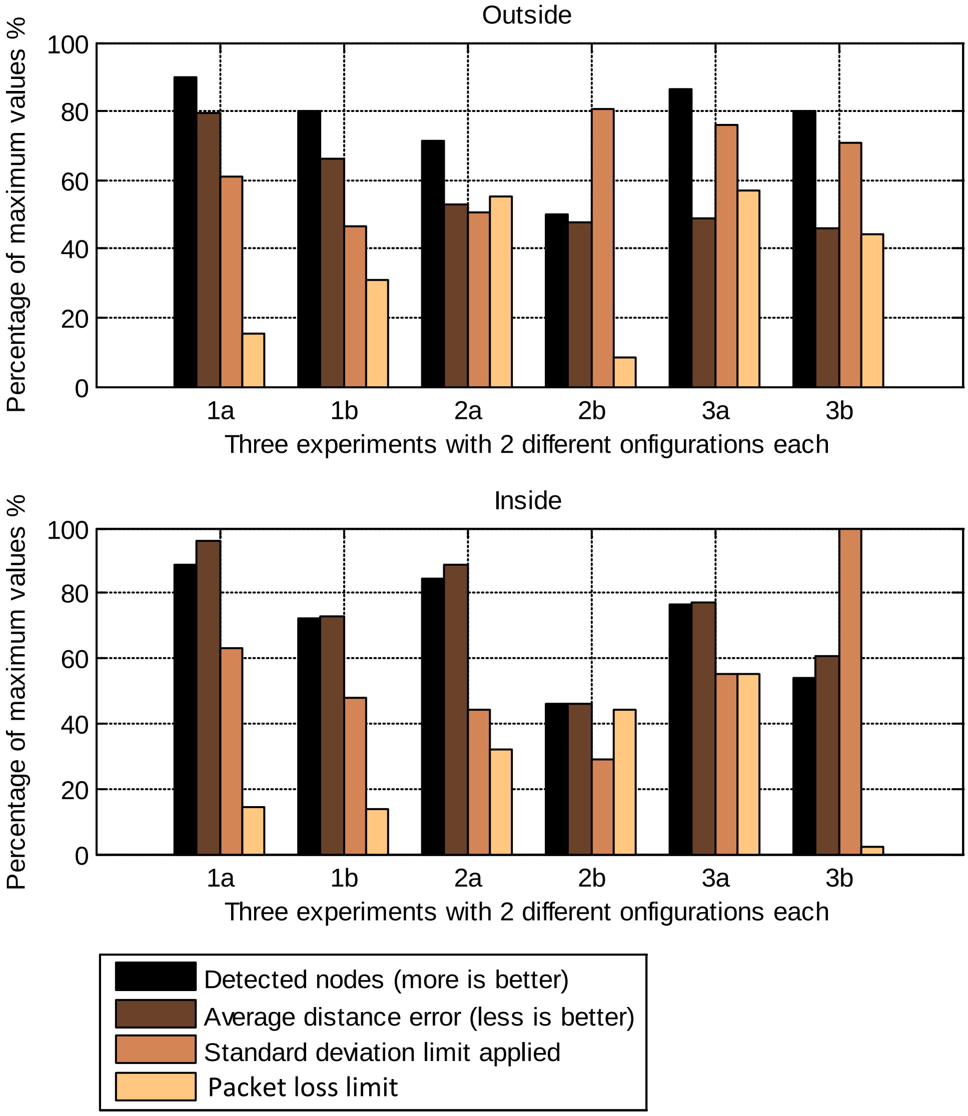

Figure 32. Percentage of average error and corresponding number of nodes using optimized SD and packet loss limits.

In Figure 32 the percentage error with the percentage of nodes that belong to that error limit are displayed along with the percentage of SD and packet loss applied as limits which have been used to achieve these results. For example the first four bars in the graph indicate one set of experiment where the error is reduced to 80 percent of the maximum error and 10 % of nodes are excluded by using 60 % of maximum standard deviation and about 18% of maximum packet loss values as limits, found in the collected RSSI data.

9. SUMMARY AND FUTURE WORK

9.1. Summary

In this thesis an improvement technique for RSSI based distance estimation for 802.15.4 sensor network is discussed. In this approach we used SD of the RSSI and the packet loss information as a part of the model parameters estimation process. The SD and packet loss limits are optimized along with the fitting curve parameters to achieve minimum distance estimation error. The distance estimator uses these optimized limits as a measure of accuracy of the remote node's estimated distance.

We proposed a simple method of finding and eliminating erroneous distance estimates by filtering the RSSI through optimized SD and packet loss limits. We conducted experiments with Sensinode NanoSeries wireless sensor nodes to collect RSSI and packet loss measurements for model parameter estimation process. We devised an optimization application to find optimal model parameters and limits. We experimentally verified the model and found that this technique does help in reducing the average distance error by identifying and eliminating only those estimates which introduce the most error.

9.2. Future Work

There are a few points which were left untouched in order to complete this thesis within required time span. Simulating the network with large number of nodes and evaluating the performance of the proposed method is one such area of interest. We intend to use the platform for integrated communications and control design, simulation, implementation and modeling (PiccSIM) for the simulation purposes.

Another area of interest is the development of improved routing algorithm which makes use of the proposed distance estimation technique to derive better and efficient routing table.

We like to make experimental performance evaluation of basic distance based localization algorithms using the proposed node-to-node distance estimation process. This study would provide a useful insight to determine the merits and demerits of the proposed method and the ways to improve it.

We need to develop a simplified version of the proposed method which is suitable to run at the wireless node without introducing much computation overhead. This would help creating a distributed localization algorithm.

REFERENCES

Aamodt K. (2006). *CC2431 Location Engine*. Application Note AN042, Texas Instruments. [Online]. Available: <http://prochild.com/board/files/tb_3/AN_042_CC2431_Location_Engine.pdf>.

Abernethy. Robert B. (2006). *The New Weibull Handbook*. 5th Ed. [online]. Available: http://www.barringer1.com/pdf/Chpt1-5th-edition.pdf

Bertoni, Henry L. (1999). *Radio Propagation for Modern Wireless Systems*, Prentice Hall Prentice Hall Professional Technical Reference.

Boukerche, Azzedine (2006). *Handbook of algorithms for wireless networking and mobile computing*. Broken Sound Parkway NW. Chapman and Hall/CRC.

Cerf, Vinton G. & Robert E. Kahn (1974). *A Protocol for Packet Network Intercommuni-cation, IEEE Transactions on Communications*, Vol. 22, No. 5, May 1974 pp. 637-648.

Contiki (2010). *Contiki Operating System web page*. [Online]. Available: <http://www.sics.se/contiki/>.

Deering, S. & R. Hinden (1998). *Internet Protocol, Version 6 Specification*. Network Working Group.

Errico , John D (2006). *Bound Constrained Optimization using fminsearch* [online]. Available: http://www.mathworks.com/matlabcentral/fileexchange/8277.

Forouzan, B.A. (2000). *TCP/IP: Protocol Suite, 1st ed*. New Delhi, India: Tata McGraw-Hill Publishing Company Limited.

FreeRTOS, 2010. *Free Real Time Operating System web page.* [Online]. Available:

<http://www.freertos.org/>.

Haykin, S. & M. Moher (2005). *Modern Wireless Communications*, Prentice Hall, ISBN 0-13-124697-6.

Huang, Shih-I & Shiuhpyng Shieh (2010). *Authentication and secret search mechanisms for RFID-aware wireless sensor networks*, International Journal of Security and Networks - Vol. 5, No.1 pp. 15 – 25.

ISO/IEC 7398-1 (1994). *Information technology -- Open Systems Interconnection – Basic Reference Model: The Basic Model*. 2nd Edition. [Online]. Available: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

Kuo, Sheng-Po , Yu-Chee Tseng, Fang-Jing Wu & Chun-Yu Lin (2005). *A Probabilistic Signal-Strength-Based Evaluation Methodology for Sensor Network Deployment.* 19th Int. Conf. on Advanced Information Networking and Applications, vol. 1, 319-324.

Lau, Erin-Ee-Lin, Boon-Giin Lee, Seung-Chul Lee & Wan-Young Chung (2008). *ENHANCED RSSI-BASED HIGH ACCURACY REAL-TIME USER LOCATION TRACKING SYSTEM FOR INDOOR AND OUTDOOR ENVIRONMENTS*, International Journal On Smart Sensing and Intelligent Systems. VOL. 1, NO. 2, 534-548.

Li, Xiaoli, Hongchi Shi , Yi Shang (2005). *A Sorted RSSI Quantization Based Algorithm for Sensor Network Localization*, Proceedings of the 11th International Conference on Parallel and Distributed Systems, p.557-563.

Linnartz. Jean-Paul (2009). *Chapter: Wireless Channels, Section: Multipath fading.* [Online]. Available: <http://www.wirelesscommunication.nl/reference/chaptr03/ricenaka/nakagami.htm>.

Montenegro, Gabriel, Nandakishore Kushalnagar, Jonathan W. Hui & David E. Culler (2007). *Transmission of IPv6 Packets over IEEE 802.15.4 Networks.* IETF RFC 4944. [Online]. Available: <http://www.ietf.org/rfc/rfc4944.txt>.

Mulligan, G. (2007). *The 6LoWPAN architecture.* In Proceedings of the 4th Workshop on Embedded Networked Sensors. 78–82. New York.

Postel, J. (1980). *User Datagram Protocol.* RFC768.

Proakis, John G & Salehi Masoud (2008). *Digital Communications*. Fifth Edition. New York etc: McGraw-Hill Inc.

Pu, Chuan-Chin & Wan-Young Chung (2008). *Mitigation of Multipath Fading Effects to Improve Indoor RSSI Performance.* IEEE Sensors Journal, Vol. 8, No. 11, November 2008, 1884 – 1886.

Radiocrafts AS (2007). *RC230x Data Sheet (rev. 1.2),* [online]. Available: <http://radiocrafts.com/uploads/rc230x_data_sheet_1_2.pdf>.

Rappaport, Theodore S (2007). *Wireless Communications: Principles and Practice*. 2nd Edition. New Jersey. Prentice Hall.

RFC793 (1981). *Transmission Control Protocol.*

Roundy S., D. Steingart, L. Fréchette, P. Wright & J. Rabaey (2004) *Power Sources for Wireless Sensor Networks,*Vol. 2920, pp. 1-17,

Saraogi, Mayank (2005). *SECURITY IN WIRELESS SENSOR NETWORKS,* Department of Computer Science University of Tennessee, Knoxville, [online]. Available: <http://www.cs.utk.edu/~saraogi/594paper.pdf>.

Srinivasan, Kannan & P.hilip Levis (2006). *RSSI is Under Appreciated*. In Proceedings of the Third ACM Workshop on Embedded Networked Sensors.

Tian, Shuang, Xinming Zhang, Pengxi Liu, Peng Sun, Xinguo Wang Li, Xiaoli, Hongchi Shi & Yi Shang (2007). *A RSSI-based DV-hop Algorithm for Wireless Sensor Networks.*

Xiao, Yang, John Paul Walters, Zhengqiang Liang, Weisong Shi & Vipin Chaudhary (2007). *Security in Distributed, Grid, and Pervasive Computing*, Auerbach Publications, pp. 367-410, [online]. Available: <http://www.cs.wayne.edu/~weisong/papers/walters05-wsn-security-survey.pdf>.

Y. Shang and W. Ruml (2004). “Improved MDS-based localization,” IEEE Infocom, Hong Kong.

Yang, Zheng & Yunhao Liu (2008), *Quality of Trilateration: Confidence based Iterative Localization*, IEEE ICDCS 2008, Beijing, China.

Zach, Shelby (2009). [online] Available: <http://6lowpan.net/wp-content/uploads/2009/12/6lowpan-book-slides-full-20091206.pdf>.

Zach, Shelby & Carsten Bormann (2009). *The Wireless Embedded Internet*, John Wiley & Sons, Ltd. [online]. Available: <http://media.wiley.com/product_data/excerpt/94/04707479/0470747994.pdf>.

Zang, Chuanzhi, Wei Liang & Haibin Yu (2007). *THE PROBABILISTIC ANALYSIS OF RSSI-BASED DISTANCE ESTIMATORS IN WIRELESS SENSOR NETWORK*, the 2007 International Conference on Intelligent Computing (ICIC). [online]. Available: <http://www.cimspaper.com/other/other1/other156.rar>.