AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

Ossi Kaltiokallio

Intrusion Detection Based on Embedded Processing of Received Signal Strength Indicator

Master's thesis for the degree of Master of Science in Technology submitted for inspection, Espoo, 11 April 2011.

Supervisor:	Prof. Heikki Koivo
Instructor:	M. Sc. (Tech.) Maurizio Bocca

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING
Department of Automation and Systems Technology

ABSTRACT OF
MASTER'S THESIS

Author: Ossi Kaltiokallio

Title: Intrusion Detection Based on Embedded Processing of Received Signal Strength Indicator

Date: 11.4.2011 Language: English Pages: 10+76

Professorship: Control Engineering

Supervisor: Professor Heikki Koivo
Instructor: M.Sc. (Tech.) Maurizio Bocca

In the context of wireless sensor networks (WSNs), the received signal strength indicator (RSSI) has been traditionally exploited for nodes localization, distance estimation, and link quality assessment. Recent research has shown that variations of the RSSI in indoor environments where nodes have been deployed can be exploited to detect movements of people. Moreover, the time-histories of the RSSI of multiple links allow reconstructing the path followed by the person inside the monitored area. This approach, though effective, requires the transmission of multiple raw RSSI time-histories to a central sink node for off-line analysis, consistently increasing latency and power consumption of the system.

This thesis aims at applying distributed processing of the RSSI measurements for indoor surveillance purposes. Through distributed processing, the nodes are able to autonomously detect and track a moving person, minimizing latency and power consumption of the system by transmitting to the sink node only the alerts raised by significant events. Moreover, a high accuracy time synchronization protocol allows the nodes to keep the radio off for over half of the time, increasing the life time of the system. During the tests, the proposed system was able to detect the intrusion of a person walking inside the monitored area, and to correctly keep track in real-time of the path he had followed.

Possible applications of such a system include surveillance of buildings, enhancement of workers safety in factories, support to emergency workers in locating people e.g. during fires and earthquakes, and to police in hostage situations or terrorist attacks.

Keywords: RSSI; embedded processing; real-time monitoring and tracking

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU
Automaatio- ja systeemitekniikan laitos

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Ossi Kaltiokallio

Työn nimi: Intrusion Detection Based on Embedded Processing of Received Signal Strength Indicator

Päivämäärä: 11.4.2011 Kieli: Englanti Sivuja: 10+76

Professuuri: Systeemitekniikka

Valvoja: Professori Heikki Koivo

Ohjaaja: DI Maurizio Bocca

Langattomien anturiverkkojen yhteydessä, vastaanotetun signaalin voimakkuuden indikaattoria (RSSI, received signal strength indicator) on perinteisesti käytetty langattomien anturien paikallistamiseen, etäisyyden estimointiin ja radiolinkin hyvyyden arviointiin. Viimeaikainen tutkimus on osoittanut, että RSSI:n vaiheluita voidaan käyttää myös havaitsemaan ihmisten läsnäolo langattoman anturiverkon läheisyydessä. Sen lisäksi ihmisen kulkema reitti valvotulla alueella voidaan uudelleenrakentaa antureiden keräämistä RSSI mittauksista. Tämä menettely on toimiva, mutta se vaatii kaikkien RSSI mittausten lähettämistä keskussolmulle erillistä prosessointia varten ja täten se kasvattaa anturiverkon latenssia ja energian kulutusta.

Diplomityön tavoitteena on käyttää RSSI mittauksia sisätilojen valvontaa varten prosessoimalla mittaukset hajautetusti anturitasolla. Hajautetulla prosessoinnilla anturiverkon solmut kykenevät itsenäisesti havaitsemaan henkilön ja seuraamaan hänen liikkeitään. Lähettämällä keskussolmulle vain hälytykset jotka liittyvät merkittäviin tapahtumiin, järjestelmän latenssi sekä energiankulutus pystytyään minimoimaan. Lisäksi järjestelmän käyttämä tarkka aikasynkronointiprotokolla mahdollistaa solmujen pitämään radionsa suljettuna yli puolet ajasta kasvattaen järjestelmän elinikää entisestään. Kokeiden aikana, esitetty järjestelmä kykeni havaitsemaan valvotulle alueelle tunkeutuneen ihmisen ja seuraamaan hänen liikkeitään reaaliajassa.

Järjestelmän mahdollisia sovelluskohteita ovat kriittisen rakennusten valvonta, työntekijöiden turvallisuuden lisääminen teollisuudessa, edesauttaa pelastustyöntekijöitä löytämään ihmiset esimerkiksi tulipaloissa ja maanjäristyksissä, sekä avustamaan poliiseja panttivankitilanteissa tai terroristihyökkäyksissä.

Avainsanat: RSSI; sulautettu prosessointi; reaaliaikainen monitorointi ja seuranta

Preface

Presented research is done as part of the Wireless Sensor Systems in Indoor Situation Modeling (WISM) project which is funded by the Finnish Funding Agency for Technology and Innovation (TEKES).

I started my first working period in the Control Engineering Group, at the Helsinki University of Technology in summer of 2008. My work was to renew a laboratory exercise and as a reward I got to try out my teaching skills when I was asked to instruct the work for the students during the fall of the same year. At the turn of the year I got my first touch on wireless sensor system as I was assigned to implement a wireless PIDplus controller for an unstable ball balancing system Halvari. For consistent continuity, I proceeded the work among wireless sensor systems as I started my Master's thesis as a part of the WISM project.

I would like to thank my instructor Maurizio Bocca for taking this exciting journey with me. During my work, I always felt the freedom to experiment yet being confidence that the direction is correct when having this remarkable scientist as my mentor. I would also like to thank my supervisor Heikki Koivo.

The work presented in this thesis is an outcome of successful teamwork and I am grateful for the entire wireless sensor systems (WSS) group of Aalto University School of Science and Technology. I would especially like to thank Emre Cosar on his persistent assistance and Joni Silvo for the many interesting discussions related to our field of research. In addition I wish to thank Olli Viitala from the Electronic Circuit Design group of Aalto University School of Science and Technology for his extensive help in carrying out the time-related measurements.

I would also like to thank my family and my fiancée for being there for me and for all the support I have received.

April 2011, Ossi Kaltiokallio

List of symbols and abbreviations

Symbols

P_s	Power of the carrier signal
d	Distance
P_{dBm}	Power of the carrier signal in dBm
P_{mW}	Power of the carrier signal in mW
t_{tick}	Tick resolution
$f_{nominal}$	Nominal frequency
$T_{overflow}$	Overflow interrupt interval
$N_{logical\text{-}clock}$	32-bit logical clock counter
t_{local}	Local time of a node
Δt	Time interval
r_{XY}	Sample correlation coefficient
x	Sample
n	Sample number
N	Total number of samples
s_k	Discrete Fourier transform coefficient
P	Expected signal strength
P_T	Transmission power
$P_{ref}(d_o)$	Measured signal strength at reference output power and distance
η	Path loss exponent
X_σ	Gaussian random variable
σ^2	Variance
e	Error
J_{iae}	Cost function
s	Size of sensitivity area
Δn	Intrusion length in samples
m	Nodes number
$v_{\perp}$	Velocity perpendicular to LoS
t_{approx}	Approximated time
v_{approx}	Approximated speed
$\Delta x_{i,j}$	Change in the measured RSSI value of link *i-j*
$f_{i,j}$	Filtered RSSI value of link *i-j*
α	Smoothing factor

$\Sigma^2_{i,j}$	Sum of squares of link *i*-*j*
m_{forget}	Forgetting factor

Abbreviations

6LoWPAN	IPv6-based Low power Wireless Area Network
AC	Access point
ACK	Acknowledgement
ACKL	Auxiliary clock
ADC	Analog-to-digital converter
BSS	Basic service set
CCA	Clear channel assessment
CPU	Central processing unit
CSMA	Carrier sense multiple access
CSMA/CA	Carrier sense multiple access/collision avoidance
CTS	Clear to send
DAC	Digital-to-analog converter
DCO	Digitally controlled oscillator
DFL	Device-free localization
DFT	Discrete Fourier Transform
DS	Distribution system
DSSS	Direct sequence spread spectrum
ESS	Extended service set
FDMA	Frequency division multiple access
FER	Frame error rate
FTSP	Flooding time synchronization protocol
GIF	Graphics interchange format
GPS	Global positioning system
HTTP	Hypertext transfer protocol
IBSS	Independent basic service set
IDU	Interface data unit
IETF	Internet Engineering Task Force
IP	Internet protocol
IPv6	Internet protocol version 6
ISM	Industrial, scientific and medical
ISS	Interrupt service routine
LAN	Local area networks

LoS	Line of sight
LQI	Link quality indicator
LR-WPAN	Low-rate wireless personal area network
MAC	Medium access control
MCKL	Master clock
MCU	Microcontroller unit
OSI	Open systems interconnection
O-QPSK	Offset quadrature phase-shift keying
PHY	Physical
PPR	Parts-per-million
PRR	Packet reception rate
QoS	Quality of service
RF	Radio frequency
RSSI	Received signal strength indicator
RTS	Request to send
SAP	Service access point
SDU	Service data unit
SMTP	Simple mail transfer protocol
SNR	Signal to noise ratio
TCP	Transmission control protocol
TDMA	Time division multiple access
TS	Time synchronization
UART	Universal Asynchronous Receiver Transmitter
UDP	User datagram protocol
USB	Universal serial bus
UWB	Ultra wide band
WLAN	Wireless local area network
WPAN	Wireless personal area network
WSN	Wireless sensor network

Table of Contents

1 Introduction

1.1 Background and motivation

Despite becoming the enduring technology for navigation and tracking purposes, the global positioning system (GPS) presents also some limitations, i.e. a null or very limited functionality in indoor environments, and the need of having the users to carry an end device at all times. Nowadays, device-free localization (DFL) and tracking of people in indoor environments could potentially be exploited in a variety of applications, such as tracking of customers in shopping malls with the aim to analyze their reaction to products and advertisements placement, detection of intruders in critical buildings or infrastructures, localization of e.g. besiegers and hostages during sieges and of civilians during fires, and to enhance workers safety in industrial halls with e.g. moving machineries. Wireless sensor networks (WSNs) represent a suitable technology to perform these tasks. A feasible solution is to extract useful information from the variations of the received signal strength indicator (RSSI) caused by the presence and movements of individuals inside the monitored area. Since in this case additional sensors such as cameras or infrareds are not used, the nodes forming the wireless network can be considered as radio frequency (RF) sensors as proposed by Patwari and Wilson (2010). Compared to traditional wired surveillance systems such as optical and infrared imaging systems, WSNs consistently reduce both the installation time and cost, and can easily be redeployed in another area of interest if needed. Moreover, the limited cost of a single device (typically less than 100 USD) makes it possible to deploy a large number of nodes covering an extensive area with a limited amount of money.

Besides being exploited for nodes localization (Sugano *et al.,* 2006 and Srbinovska *et al.*, 2008), distance estimation (Faheem *et al.*, 2010 and Benkic *et al.,* 2008), and link quality assessment purposes (Tang *et al.,* 2007 and Srinivasan *et al.,* 2006a), the RSSI has shown to be useful also for detecting movements of individuals inside an area monitored through a WSN (Wilson and Patwari, 2010a and Zhang *et al.*, 2007). In a static environment, the RSSI measurements are nearly constant as shown by Srinivasan *et al.* (2006b). On the contrary, when the conditions inside the network change, the variance of the RSSI measurements increases. By monitoring the changes of the RSSI over multiple links, it is then possible to create a virtual RF grid through which to detect and track moving objects inside the monitored area.

1.2 Scope and objectives

The scope of this thesis is to design and develop a real-time device-free localization (DFL) system that exploits radio signals to detect the presence of individuals. The system is used for positioning individuals and to track their movements in indoor environments. In addition, the aim is to investigate the characteristics of radio signal propagation in indoor environments and to study how the presence of people influences radio signal propagation.

The main objective of this thesis is to design a DFL system that is easily re-deployable, remotely reconfigurable, easy to use, and operates in real-time. In addition, the detection of humans is to be done locally in the nodes, so that only significant events related to intrusions are transmitted to a central base station, therefore minimizing the communication overhead of the network. The embedded intrusion detection algorithm is designed so that it is able to cope with the limited resources, in terms of computational power and available memory space, of the microcontroller unit (MCU) found in the nodes.

1.2.1 System requirements

In this thesis, an embedded algorithm that processes the RSSI measurements locally in the nodes and detects the intruder obstructing the line of sight (LoS) between communicating nodes is developed and implemented. The algorithm is designed so that it does not depend on the characteristic of the surrounding indoor environment and so that it does not include hard coded thresholds. In addition, the algorithm is designed so that it does not require training of the network in static conditions (i.e. when movement is not present inside the monitored area). The link obstructions caused by the intruder are notified to a central base station and then exploited to estimate the intruder's position. The path of the intruder is tracked from the consecutive position estimates and the tracking application provides a reliable estimate of the intruder's position and trajectory in real-time with minimal latency. In addition, the nodes keep their radio off when ever scheduled communications are not expected increasing the network lifetime.

1.3 Contributions

Contributions of the author in the thesis are listed as follows:

- A device-free, wireless, real-time, intrusions detection and tracking application for indoor environments is developed and tested. The proposed system is based on monitoring the changes in the RSSI caused by a person moving among or in the close proximity of communicating low-power sensor nodes, operating in the 2.4 GHz industrial, scientific and medical (ISM) band.

- A comprehensive study of the radio channel and signal strength characteristics in indoor environments is performed to gain insight of the wireless medium. The results introduce design aspects for a RF based DFL system.
- An embedded algorithm is developed to detect the presence of a person moving among or in the close proximity of communicating nodes. The embedded algorithm enables transmitting to a central base station only the information regarding significant events (i.e. alerts), therefore minimizing the communication overhead and latency of the system.
- A high accuracy time synchronization (TS) protocol is exploited to enable time division multiple access (TDMA) communication schedule among the nodes, increasing the tolerance of the network to nodes failure. The TS protocol allows also disabling the radio of the nodes when scheduled transmissions are not expected, leading to an increment of the network lifetime.
- A method to transmit efficiently the alerts to the central base station without increasing the communication overhead is introduced. In this way, latency of the intrusion detection system is minimized, enabling real-time tracking of the intruder. Besides, by excluding additional communications, the power consumption of the system is further reduced.
- When node positions are known a priori, the alerts transmitted by the nodes forming the RF sensor network enable position estimation and tracking of the intruder. An estimate of the current position is calculated by applying one of four different methods developed in this thesis. The accuracy of the real-time tracking application is increased by combining the most recent position estimates.
- The embedded RSSI intrusion detection algorithm and the real-time tracking application were tested in the entrance hall of a university building, with a WSN consisting of 12 nodes and the sink node. The tests were conducted using two different network layouts and two different node intervals.
- O. Kaltiokallio, M. Bocca, and L. M. Eriksson, “Distributed RSSI Processing for Intrusion Detection in Indoor Environments,” in Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN ’10), Apr. 2010.
- M. Bocca, O. Kaltiokallio, and J. Silvo, “Real-Time and Reliable Wireless Sensor Networks for Smart Wireless Automation Applications,” accepted to the Automaatio XIX seminar, Mar. 2011.

The work described in this thesis is the result of the effort of a group of people. In the following, the people who have contributed to different aspects of the work are presented.

The sensor networking platforms used throughout the experiments were for most parts put together and maintained by Viktor Nässi. The system presented in this thesis exploits a medium access control (MAC) layer TS protocol, originally implemented by Mahmood and Jäntti (2009). The protocol was initially implemented on a different hardware and it has recently been ported to the platform used in the thesis by Bocca *et al.* (2011). The application to measure the background noise of the radio channels and to rank the radio channels was developed by Maurizio Bocca. The power consumption measurements were conducted by Ossi Kaltiokallio and Maurizio Bocca. The time synchronization accuracy and run-time measurements of the application were conducted by Ossi Kaltiokallio with the help of Olli Viitala. The embedded algorithm to detect the intrusions was developed by Ossi Kaltiokallio under supervision of Maurizio Bocca and with the help of Lasse Eriksson. The other parts of the development, tests, and analyses were done by Ossi Kaltiokallio.

1.4 Structure

The thesis is structured as follows. Chapter 2 provides an overview of wireless sensor networks, introduces the communication stack of the sensor nodes and the main phenomena affecting the wireless medium, and lists the related work. In chapter 3, after describing the sensor networking platform used in the experiments, the exploited TS protocol is introduced. At the end of the chapter the radio channel characteristics and causes for RSSI variabilities are introduced. Chapter 4 presents the developed intrusion detection and tracking application, i.e. the embedded algorithm executed locally in the nodes to detect intrusions, four different methods to estimate the position of the intruder, and the real-time tracking application. The system is experimentally evaluated at the end of the chapter in four network setups. In the final chapter, conclusions and key observations of the thesis are summarized.

2 Wireless sensor networks

A WSN consists of spatially distributed autonomous devices which communicate with one another exploiting a wireless medium. Each node typically consists of a RF transceiver, a MCU, an external power supply, and various types of sensors used to measure the surrounding environment. Initial research in the area of WSNs was mainly driven by military applications (e.g. Smart Dust (Kahn *et al.*, 2000)) (Römer and Mattern, 2004). Nowadays, WSNs are utilized for various purposes such as environmental monitoring (Hasler *et al.*, 2009), structural health monitoring (Ceriotti *et al.*, 2009 and Bocca *et al.*, 2009), precision agriculture (Dong *et al.*, 2010), etc.

The following sections cover fundamental issues related to WSNs. The chapter starts by introducing three different short range wireless communication standards and since the sensor networking platforms used in this thesis are based on the IEEE 802.15.4 standard, protocols of the standard are examined in more detail. In section 2.3 basic multiple access methods are introduced, and in the following section different network topologies are presented. The communication stack, which defines the interconnections of the wireless devices, of IPv6-based low power wireless area network (6LoWPAN) is examined and it is compared to the open systems interconnection (OSI) model in section 2.5. Section 2.6 covers the characteristics of the wireless medium and phenomenon’s affecting radio signals. Work related to detecting and tracking movement of individuals with RF networks is discussed at the end of the chapter.

2.1 Short range wireless communication standards

There is a range of technologies enabling wireless connectivity, each designed for distinct purposes. Some technologies emphasize bandwidth, whereas others call for low power consumption or inexpensive devices. Each standard is designed for some specific purpose in mind and rather than being competing technologies, they are complementary for one another, each best suitable for a specific application. In the following sections three different short range wireless communication standards are introduced. Summary of the standards including ZigBee is shown in Table 1.

2.1.1 Bluetooth

Bluetooth is a low-power radio technology designed for short range and inexpensive devices. The technology was developed by Ericsson in 1994 and it has become the standard wireless solution for cordless computer accessories and mobile phone peripherals (Bluetooth, 2010). Its physical (PHY) layer and MAC layer are defined within the IEEE 802.15.1 protocol (IEEE 802.15.1, 2010). Bluetooth defines two different connectivity topologies: piconet and scatternet. A piconet is a wireless personal area network (WPAN) consisting of one master device and up to 7 active slave devices. The master node is used to synchronize the global clock of the network which is then used for frequency hopping. Communication is performed under the control of the master node. The slave nodes are able to communicate only to the master node in a point-to-point fashion, while the master node can transmit using point-to-multipoint broadcasts (Lee *et al.*, 2007). Multiple piconets form a scatternet where the adjacent piconets are connected via a slave node. A slave node can be a part of multiple piconets, while a master node can be a slave at another piconet. However, a node cannot be a master in multiple piconets. Suitability of Bluetooth in wireless sensor networks is studied e.g. by Leopold *et al.* (2003).

2.1.2 Wireless local area network (WLAN)

WLAN has been developed to replace the cables typical of local area networks (LANs). WLAN networks exploit radio technologies defined in the IEEE 802.11 standard providing secure, reliable, and fast wireless communication at the expense of being complex and power hungry (IEEE 802.11, 2010). WLAN networks operate in the 2.4 GHz and 5 GHz frequency bands providing a bandwidth of 2-540 Mb/s (Wi-Fi Alliance, 2010). IEEE 802.11 offers two different network configurations: independent basic service set (IBSS) and extended service set (ESS) (Ohrtman and Roeder, 2003). The IBSS is a group of working stations communicating directly to one another without the existence of an access point (AC). A set of working stations form a basic service set (BSS) which can access the distribution system (DS) via the ACs. The DS forms the backbone of the network and it is usually an Ethernet. Multiple BSSs connected together through the DS form the ESS network configuration.

2.1.3 Ultra-wideband (UWB)

UWB differs greatly from the other two radio technologies introduced above, being an impulse based radio solution. UWB utilizes a very broad portion of the radio spectrum, overlapping other radio technologies. The transmissions however use a very low signal energy level (-41.3 dBm/MHz) that does not interfere with co-existing narrowband radios, e.g. ZigBee and Bluetooth (WiMedia Alliance, 2010). UWB offers a short-range high-speed wireless communication reaching a bandwidth of over 110 Mb/s (up to 480 Mb/s), which can fulfill the rapid transfer requirements of bandwidth intensive files such as audio and

Table 1: Comparison of short range radio protocols (Lee *et al.*, *2007*)

	Bluetooth (802.15.1)	**UWB (802.15.3a)**	**ZigBee (802.15.4)**	**WLAN (802.11a/b/g)**
Frequency band	2.4 GHz	3.1 – 10.6 GHz	868/915 MHz, 2.4-2.4835 GHz	2.4 GHz; 5 GHz
Max. signal rate	1 Mb/s	110 Mb/s	250 Kb/s	54 Mb/s
Nominal range	10 m	10 m	10 – 100 m	100 m
Nominal TX power	0 – 10 dBm	-41.3 dBm/MHz	(-25) – 0 dBm	15 – 20 dBm
Number of RF channels	79	1 – 15	1/10/16	14 (2.4 GHz)
Channel bandwidth	1 MHz	500 MHz – 7.5 GHz	0.3/0.6/2 MHz	22 MHz
Modulation type	GFSK	BPSK, QPSK	BPSK(+ASK), O-QPSK	BPSK,QPSK, CCK, M-QAM, COFDM
Spreading	FHSS	DS-UWB, MB-OFDM	DSSS	DSSS, CCK, OFDM
Coexistence mechanism	Adaptive frequency hopping	Adaptive frequency hopping	Dynamic freq. selection	Dynamic freq. selection, transmit power control
Basic cell	Piconet	Piconet	Star	BSS
Extension of the basic cell	Scatternet	Peer-to-peer	Cluster tree, Mesh	ESS
Max number of cell nodes	8	8	>65000	2007

video. Also there has been discussion on UWB possibly replacing high speed serial buses such as universal serial bus (USB) 2.0 and FireWire (Lee *et al.*, 2007).

2.2 IEEE 802.15.4 protocols

IEEE 802.15.4 is a standard for low-rate wireless personal area networks (LR-WPAN's), which specifies the PHY and MAC layers of the communication stack. The protocol is a basis for such wireless communication standards as WirelessHART, ZigBee, and

6LoWPAN, which all offer the upper layers of the communication stack. The standards intention is to offer devices with low cost, low power consumption, and low complexity.

2.2.1 WirelessHART

WirelessHART is a wireless communication standard designed for measurement and control applications in process plants. A WirelessHART network consists of three basic elements: wireless field device, gateway, and network manager. Field devices are used for process monitoring and control, whereas a gateway enables the communication between the field devices and a host application that is connected to an automation system bus. A network manager is responsible for network configuration, scheduling, route management, and network health monitoring. All devices in the network can act as routers in the wireless network and the network manager is in most cases integrated to the network gateway. The network uses IEEE 802.15.4 compatible radios for communication, and it enables a mesh network design for robust and redundant communication. (HART Foundation, 2010)

2.2.2 ZigBee

ZigBee is a higher layer communication protocol built on top of the IEEE 802.15.4 standard for LR-WPANs. ZigBee Alliance developed the ZigBee protocol to add the network, security and application software to the existing IEEE 802.15.4 standard (ZigBee Alliance, 2010). ZigBee is optimized for automation sensor networks, where there is no need for high bandwidth, but low power consumption, low latency and high quality-of-service (QoS) are required (Eriksson *et al.,* 2008). The technology supports mesh networks consisting of at most 2^{16} = 65536 devices co-operating with one another. There are three different types of ZigBee devices: coordinators, routers and end devices. A ZigBee coordinator is responsible for network formation, data storage, and linking networks together. The router enables multi-hop communication across devices and also links device groups together. A ZigBee end device consists of possible sensors and actuators that interact with the surroundings; the end device communicates only with router or coordinator devices (Yick *et al.,* 2008).

2.2.3 6LoWPAN

6LoWPAN is a low power wireless personal area network protocol that is based on the internet protocol version 6 (IPv6). The aim of the protocol is to provide low-power radio communication that exploits the internet protocol (IP) addresses to enable internet connectivity. For the 6LoWPAN communication stack, an adaptation layer is defined to compress, fragment, and reassemble IPv6 headers and to enable mesh route forwarding. The adaptation layer is a standard proposed by the internet engineering task force (IETF). Because of the IP based communication, 6LoWPAN's can be connected to other networks (e.g.

WLAN, Ethernet, etc.) based on IP addresses via border routers that forward IP based packets between the different media. (Shelby and Bormann, 2010)

2.3 Multiple access methods

The nodes of a WSN share a common medium for communication, and without proper management of the medium, communication would be inefficient. Packet collisions would occur and packet delivery could not be assured within a certain time interval. Also the channel would be occupied most of the time with unnecessary retransmissions, due to improper management in the first place. Another point of view is that the whole capacity of the medium is not needed by one communication pair in the network, and the shared medium could also be used by other nodes. The channel division for multiple users is called multiple access and it provides the methods to manage the limited resources of the radio channel efficiently.

The multiple access methods can be classified into two distinct categories: conflict-free and contention protocols (Rom and Sidi 1990). Conflict-free protocols are not interfered by other transmission, and when a transmission is made it is ensured that it is successful. A conflict-free transmission can be assured by allocating the channel for the users either timely wise, frequency wise, or by a combination of the two. In TDMA, a single user is given the whole bandwidth for a fraction of time, where as a single user is given a fraction of the bandwidth for the entire time in frequency division multiple access (FDMA) as shown in Figure 1. In contention protocols a transmission is not guaranteed to be successful, and the protocols must determine a routine to solve conflicts so that in the end the transmission can be assured. The benefit of contention based protocols is that idle users do not consume the

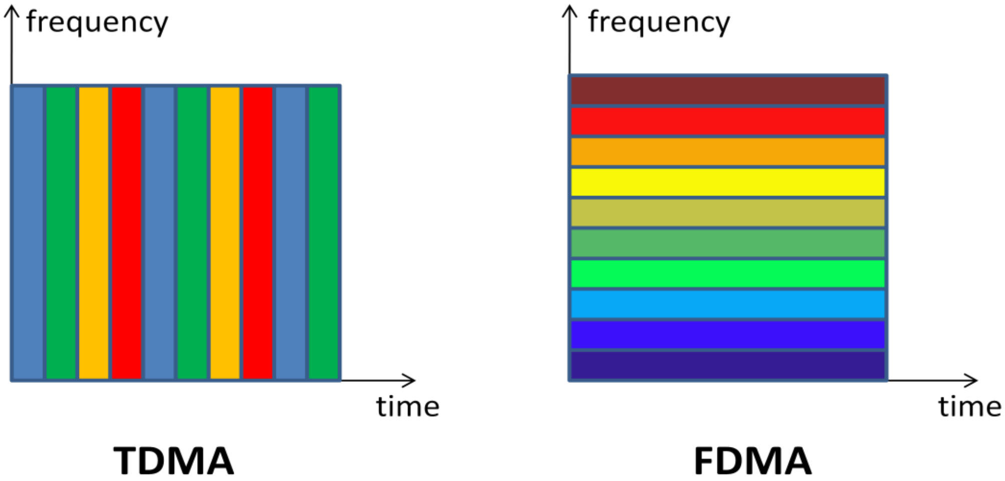


Figure 1: Channel allocation in respect to time and frequency by TDMA and FDMA techniques.

scarce resources of the radio channel. An example of a contention protocol is carrier sense multiple access (CSMA).

2.3.1 Time division multiple access

In the TDMA protocol the time axis is divided into super frames, also denoted as cycles or frames. Each super frame is divided into smaller time slots, and each node in the network is assigned a time slot that they can use. During the time slot the whole bandwidth is devoted to that one node. The cycles are periodic and each node has the same time slot in each frame. In order to exploit TDMA, the network has to be synchronized, so that each node in the network knows when they are allowed to transmit and when they should expect packets from other nodes. Since the time instances for communication are known, the nodes are able to turn off their radio to conserve power when scheduled communications are not expected. Downsides of TDMA are that it introduces communication delay and it is also inefficient since it allocates the whole bandwidth for the assigned slot of time (Tuononen, 2009).

2.3.2 Frequency division multiple access

The FDMA protocol resembles TDMA, but instead of dividing the time space, it separates the frequency band to smaller portions called sub-bands or channels. Each node in the network is assigned a distinct channel to operate on, and in this way every user is guaranteed a constant bandwidth at all times. This aspect is advantageous in applications where minor communication delays are permitted, and the throughput has to be guaranteed. The disadvantage of FDMA is that the channel is occupied at all times by the user even though no transmissions are made, decreasing the efficiency of the channel. Another downside of the technique is caused by the limited number of channels available which decreases the scalability of the network (Eriksson *et al.,* 2008). Figure 1 presents the division of time and frequency space corresponding to TDMA and FDMA protocol.

2.3.3 Carrier sense multiple access/collision avoidance

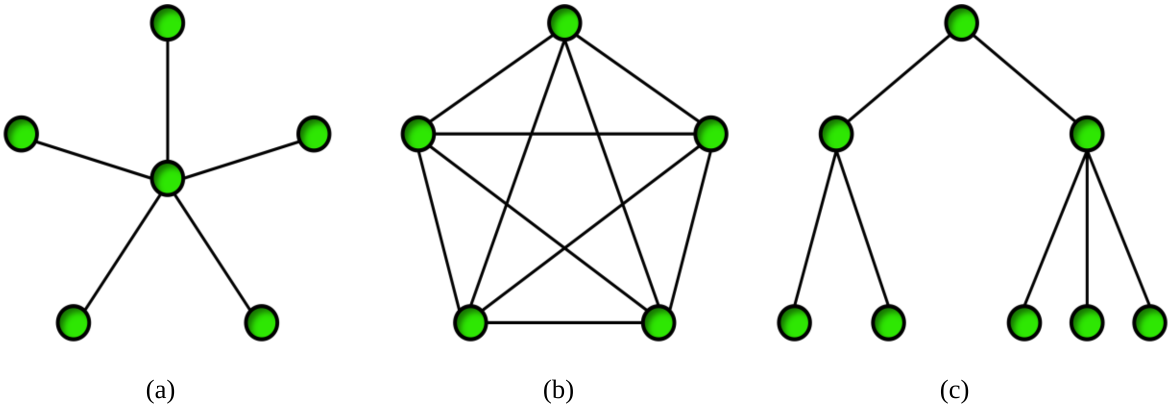
Carrier sense multiple access with collision avoidance (CSMA/CA) is a contention based multiple access method which does not depend on a coordinator device to manage the channel. The underlying concept is that the transmitting nodes listen to the channel before communication and if the channel is sensed to be idle a transmission can be successfully made. If the medium is sensed to be busy, the transmission is delayed to a later time instance. The CSMA/CA protocol is a widely adopted technique in wireless networks (Ha *et al.*, 2007).

The collision avoidance in the CSMA/CA is maintained with a handshake routine between the communicating nodes. Before transmission of a data packet, a source node asks permission for transmission from the receiver by sending a short request to send (RTS) packet. If the destination receives the RTS packet correctly, it corresponds to a situation where it is not receiving packets from other nodes at the time. The receiver acknowledges the RTS with a clear to send (CTS) packet, and if received correctly at the source node the actual data packet is sent. After transmitting the data packet the source node waits for an acknowledgement (ACK) message from the receiver. If CTS is not received upon a certain time period, the source assumes that the packet has collided and a retransmission is attempted after a random backoff period. A backoff period is also launched in situations where the source senses that the channel is busy. (Kumar *et al.*, 2008)

2.4 Network topology

Network topology is defined as the conjunction of various nodes in the wireless network and it is one of the key design factors of WSNs (Eriksson *et al.*, 2008). The network topology effects heavily on communication traffic, QoS, power consumption of the network, and complexity of the realization. Three basic network topologies are the star, mesh and tree topology and they are described below in respective order. It is also possible to combine various topologies in different parts of the network to utilize the desirable features of each topology.

In wireless networks with a star topology, each node of the network communicates solely to a central node in a point-to-point fashion. The central node may act as a repeater or as an access point to the network. Advantage of the star network is its simplicity, but its disadvantage is its intolerability to failures. If the central node dies the whole network collapses. A star topology is presented in Figure 2 (a).



(a) (b) (c)

Figure 2: Three distinct network topologies: star (a), mesh (b), and tree (c) topology.

In a mesh topology, depicted in Figure 2 (b), every node in the network can act as a router and packets can be delivered from the source to the destination via multiple routes. The mesh topology is said to be fully connected, meaning that each node is connected to every other node in the network. Mesh topology provides robustness to the network, since broken links can be replaced by a compensatory path, supposing that there is more than one node within the communication range. A drawback of the mesh topology is the relatively heavy routing protocol.

A tree topology is a hierarchical structure consisting of a root node and lower level nodes (i.e. children). The root node forms the top level of the hierarchy and it can have one or multiple children. These children constitute the second level of the tree, and they act as the parents for the third level nodes. Each node in the tree has exactly one parent, excluding the root node, and possibly multiple children. A tree topology must have at least three levels of hierarchy, since otherwise it would form a star. The routing protocol of the topology can be made relatively light and the number of point-to-point connections is one less than the number of nodes (cf. $m \cdot (m-1)/2$ for a fully connected mesh topology, where m is the number of nodes). As in a star network, a tree topology is also vulnerable to broken links, where a link failure high in the hierarchy can cause whole portions of the network to collapse.

2.5 The OSI reference model and the 6LoWPAN protocol stack

To interconnect various systems between each other they need a way to communicate that is standardized. An example of such a standard is the OSI reference model which consists of seven layers to reduce complexity of the communication stack. Every layer of the communication stack offers its services to the layer above it; the lower layer is referred to as the service provider, whereas the higher layer as the service user. For the higher layer to access services of the layer below, each layer is provided with a service access point (SAP) excluding the physical layer which is the lowest layer in the stack. The upper layer isn’t conscious of how the services are implemented in the layer below, it is only aware of the interface data unit (IDU) passed through the SAP. The IDU is normally made up of a service data unit (SDU), which is the actual data, and the associated control information.

Upon packet transmission, the highest layer (i.e. application layer) attaches its own header information to the actual data packet and delivers it to the layer below. Once the data packet is received at each layer in the model, the intermediate layers append their own unique header information to the packet and forward the packet to the layer below. This procedure continues until the packet reaches the lowest layer (i.e. physical layer), where the data packet is actually transmitted using the physical medium (optical fiber, pair cable, air).

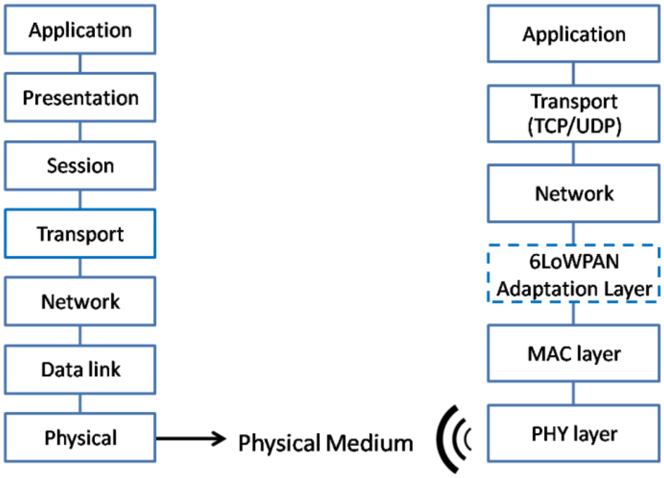


Figure 3: The seven layers of the OSI reference model on the left and the 6LoWPAN communication stack presented on the right.

Upon reception at the destination side, the process is reversed. Each layer extracts the header information from the packet and passes the data to the layer above. The procedure continues until the data packet reaches the highest layer (i.e. application layer). (Siva Ram Murthy and Manoj, 2004)

2.5.1 Layer assignments of the OSI reference model

The seven layers of the OSI reference model are presented in Figure 3 on the left, and in the following, assignments of each layer are briefly presented. The layers of the model are explained in more detail e.g. in Siva Ram Murthy and Manoj (2004), and in Stallings (2005). Application layer acts as the interface between the end-user's application and the communication stack. The layer also provides distributed information services. Examples of protocols that implement the application layer include simple mail transfer protocol (SMTP) and hypertext transfer protocol (HTTP).

Presentation layer is concerned with the syntax and semantics of the data interchanged between the two various end systems. The computers might use different syntax to represent the data, and the presentation layer ensures that the packages used to wrap the data have a common outlook. Examples of presentation layer protocols are different file formats such as graphics interchange format (GIF). The session layer provides the control mechanism for applications to communicate with one another. This includes establishment, management and termination of sessions. Examples of session layer protocols are scarce since the OSI reference model was never adopted as it was designed, but one such a protocol is AppleTalk developed by Apple.

The fourth layer of the OSI reference model is the transport layer which provides the higher layers a network independent interface to the lower layers. The layer is responsible for end-to-end error recovery, flow control, and partitioning and reassembly of messages. Transmission control protocol (TCP) and user datagram protocol (UDP) are examples of transport layer protocols. The layer below is the network layer which is responsible for assignment of destination addresses, routing, and management of network connections. IP is an example protocol of the network layer.

Data link layer offers reliable transfer of data across the physical medium. The data are, if large enough, divided into smaller frames before transmission. Also there is a mechanism for detecting and retransmission of lost and damaged packets. In networks that utilize a shared medium (e.g. wireless networks) the data link layer is also used to control the medium access as explained in section 2.3. The lowest layer of the OSI reference model is the physical layer, which is the interface to the used physical medium. The layer is liable for the transmission of the bit stream of 0's and 1's over the physical medium. It handles the mechanical and electrical specifications of the network hardware and the physical transmission medium to be used for the transmission. An example of the physical layer is the Ethernet.

2.5.2 Layer assignments of the 6LoWPAN protocol stack

The 6LoWPAN communication stack is almost identical with the IP based protocol stack defined by the Network Working Group of the IETF (RFC1122, 1989). However there are some differences such as: 6LoWPAN only supports IPv6, the most common transport protocol is UDP, and application protocols are mostly application specific. In the following, the lowest layers, defined by the IEEE 802.15.4 standard, are explained briefly. One can refer to Shelby and Bormann, (2009) for a more detailed review of the 6LoWPAN protocol.

The physical layer manages the RF transceiver and it provides the data transmission and reception service. The layer is responsible e.g. activation and deactivation of the RF transceiver, providing clear channel assessment (CCA), and channel and transmission power selection. The physical layer, of the original IEEE 802.15.4 2003 standard offers three distinct frequency bands: 868 MHz, 915 MHz, and 2400-2483.5 MHz, all based on the direct sequence spread spectrum (DSSS) modulation technique. The gross data rates of the frequency bands in respective order are: 20 kbit/s, 40 kbit/s, and 250 kbit/s. The MAC layer provides an interface between the higher layers and the PHY layer, and it is responsible e.g. device association, access to the physical radio channel, supporting device security, and generation and synchronization of network beacons. The MAC layer controls the medium access by CSMA-CA. (IEEE 802.15.4, 2010)

2.6 The wireless medium

Wireless sensor networks deploy radio waves as the physical means to transmit data. Radio signals are a type of electromagnetic radiation with a certain amplitude, frequency, and wave length. In ideal circumstances (e.g. free space, vacuum), the phenomena effecting radio signal propagation (e.g. distance attenuation) are well known. However, most of the wireless networks are deployed in real-world environments, where the wireless communication channel is exposed to multiple phenomena that have a negative impact on it. Such phenomena, to name the most common, include: multipath, distortion, power loss, fading, shadowing, noise and interference. In the next section, a few of these phenomena's are explained.

2.6.1 Phenomena effecting the wireless communication channel

Power loss refers to the decaying energy of the carrier signal, which is caused by damping in the medium (Stallings, 2004). The energy of the carrier signal deviates to a sphere surface once the signal is broadcasted from the antenna. The surface of the sphere is proportional to the square of the distance from the antenna and this formulation sets a relation between the signal power and the distance from the transmitting antenna as follows:

$$P \sim \frac{1}{d^2} \tag{1}$$

where P is the power of the carrier signal and d is the distance from the transmitter antenna.

Multipath is a phenomenon in which a transmitted signal travels via multiple routes from the transmitter to the receiver (Eriksson *et al*., 2008). The traveled distance is different for every signal and because of this, the signals are not received simultaneously and phase difference results into interference. Multipath can be caused by three different phenomena's: reflection, diffraction, and scattering. Reflections are caused by the carrier signal bouncing of obstructions. Diffraction can result when the radio signal encounters an obstacle, and it can be described as the bending of radio signals around small objects and the spreading of radio waves past small openings. Scattering is a physical phenomenon in which the carrier signal changes the direction of propagation due to the non-homogenous medium it travels through.

Fading in a wireless communication channel is caused by the above mentioned multipath effect and it can be divided into two categories: the Doppler spread and the delay spread (Zhang et al., 2003). The Doppler spread is caused by the movement of the receiver or the transmitter, which causes a change in the absolute velocity of the signal. The delay spread is caused by the changes in the close proximity environment. For example, a person who walks in the close proximity of the transmitting node causes multipath to change dynamically causing variation in the received signal power, a phenomenon referred as multipath fading. Correspondingly a person who is in between a communicating node pair can cause strong attenuation in the signal and this is referred as shadowing (Patwari and Wilson, 2010).

Interference is generally referred to as the unwanted additive disturbance to the transmitted signal and it can be divided into two classes: adjacent channel interference and co-channel interference (Siva Ram Murthy and Manoj, 2004). In the adjacent channel interference, signals in nearby frequencies have components outside their allocated bandwidth, and these components can interfere with the communication on neighboring frequency bands. Co-channel interference is due to other systems using the same transmission frequency. Possible sources of co-channel interference are networks operating on the same channel (e.g. WLAN). Most wireless sensor nodes are highly sensitive to interference, because of the low-power radio and it can result to packet drops and data errors, which can in the worst case, weaken the performance of the network.

2.6.2 Received signal strength indicator (RSSI)

In wireless communications, RSSI is a measurement of the signal strength in the received radio signal. The RSSI measurement provided by the RF transceiver is unitless, where the maximum value depends on the supplier and the range of RSSI values provided by the vendor is relative to the actual power, which is expressed in mW or dBm. However, each supplier provides their own accuracy, scale, and offset level for the measurement. The RSSI measurement of the CC2420 RF transceiver is described in more detail in section 3.1.2.1.

The RSSI measurement is the relative power in decibels (dBm) to the measured power referenced to one milliwatt (mW). Zero dBm corresponds to one mW, and to double the power means an increase of roughly 3 dBm. Respectively, to decrease the power in half is analogous to lowering the power by -3 dBm. The power in dBm can be expressed as a function of the power in mW as follows:

$$P_{dBm}=10\ log_{10}\, P_{mW}, \tag{2}$$

where P_{dBm} is the power in dBm and P_{mW} is the power in mW. Table 2 shows the dependency between decibels and watts, and examples of radio technologies operating on different output power levels.

In recent years, RSSI has attracted a lot of attention in the area of wireless communication and WSN research. The reason for this is that the measure is a standard feature in most

Table 2: Typical output power levels of different radio technologies [Wikipedia dBm, 2010]

dBm	Power	Example
80	100 kW	Transmission power of a FM radio station with a range of 50 km
33	2 W	Maximum output power from a UMTS/3G mobile phone
20	100 mW	Transmission power of Bluetooth Class 1 radio, range 100 m
15	32 mW	Nominal WLAN transmission power of a laptop
4	2.5 mW	Transmission power of Bluetooth Class 2 radio, range 10 m
0	1 mW	Transmission power of Bluetooth Class 3 radio, range 1 m
-10	100 µW	Typical maximum received signal power of WSNs
-70	100 pW	Typical received signal power range of a WLAN

radios, so additional sensors are not needed. In addition, it doesn't require additional power consumption. The use of RSSI is extensive as it has been utilized for radio link quality assessment (Srinivasan and Levis, 2006a,), nodes localization (Zanca *et al*., 2008), surveillance applications (Hussain *et al*., 2008), packets reception rate modeling (Srinivasan *et al*., 2006b), and transmission power control (Lin *et al*., 2006).

Despite the vast usage of the RSSI, the dynamics of this measurement are still difficult, if not impossible, to predict or model. Many parameters can influence the measure: in addition to multipath, fading, and shadowing, the transmitter and receiver variability, as well as the antenna orientation, can impact the measured RSSI value (Lymberopoulos *et al*., 2006). Moreover, the nodes spatial displacement and the surrounding environment contribute to RSSI variation.

2.7 Related work

Several studies have already demonstrated that the RSSI can be exploited to detect the presence of a person and to track its path inside an area monitored by a WSN. Hussain *et al*. (2008) proved that RSSI measurements can be used to detect an intruder located between two sensor nodes. To emulate a real life situation, the experiments were conducted in a standard living room, using various node distances. A beam of light traveling from one node to the other was used to record the exact times of LoS crossings. The results (conducted with MICAz nodes operating in the 2.4 GHz band), showed a high level of correlation between the alerts raised by a RSSI-based intrusion detection algorithm and the LoS crossings of the radio link detected by the beam of light. Also at high distances (7 meters), the level of correlation and the significance between the RSSI measurements and the light beam remained high ($r^2 > 0.35$ and p-value < 0.00001).

The use of the RSSI to detect motion and estimate velocity was investigated by Woyach *et al*. (2006). This work (conducted with MICA2 nodes operating at 433 MHz and MICAz nodes operating in the 2.4 GHz band) showed that a moving person causes multipath fading and shadowing of the radio signal. The experiments were conducted by placing two transmitter/receiver pairs of nodes 6 m apart from each other and elevated 0.5 m from the floor. The transmitter and receiver nodes of one link were 1.5 m apart from each other. The RSSI measurements of each link were forwarded to a base station for offline analysis. The results indicated that the LoS crossings of a moving person can be identified by both links. When the positions of the nodes are known, by comparing the time stamps between subsequent shadowing events it was possible to estimate the speed of the person.

Wilson and Patwari (2010a) exploit the RSSI to estimate the positions of people inside an area surrounded by a wireless network. This is done by tracking the changes in the network attenuation field caused by the presence of people. In their work (conducted with TelosB nodes operating in the 2.4 GHz band) the system is first calibrated in static conditions, i.e. when the monitored area is free from moving objects. During run-time, the calibration results are used to derive the differences in the RSSI measurements caused by the presence and movements of people, and Tikhonov regularization is applied to estimate the positions of people. The experiments were conducted by deploying 28 nodes all around a squared surface covering 41 m^2. Eight nodes were positioned at each side of the square. The network used a token passing communication protocol, in which only one node at a time broadcasted a packet while all the other nodes listened, after which the transmission turn was passed to the next node. The receiver examined the sender ID and added its RSSI measurements to the packet it broadcasted. The base-station node listened to the network communication at all times and gathered the RSSI measurements of each link to a laptop computer. Imaging the locations of humans was obtained from the combined RSSI measurements of the network.

In (Wilson and Patwari, 2010b), the statistical attenuation model and the variance of the attenuation field are exploited to estimate the spatial coordinates of a person. In addition, a Kalman filter is applied on data previously collected in order to track the coordinates of a moving person. In the experiments, 34 nodes were deployed around a typical home. The communication procedure was equivalent to the one in (Wilson et al., 2010a). In the work, dense walls prevent many of the links from experiencing significant attenuation caused by the presence of a human. In fact, it was shown that many links experience an increase in signal strength when LoS between nodes was obstructed. From this, it was concluded that the average of the signal strength is an unpredictable measure to estimate the position of a person. However, variance was found to be a more reliable measure to identify object movements between the links. During the experiments, a person moved inside the building and the path was tracked with an average error of 1.03 m. Most of the tracking error resulted from the lag introduced by the Kalman filter, but also from delays due to measurements collection and processing. Without these delays, the average error between the estimated and real positions was 0.45 m.

Zhang *et al*. (2007) propose a RF sensor network composed of MICA2 nodes operating at 870 MHz to track a moving person in an indoor environment. The measurements were conducted with 16 nodes elevated to a height of 2.4 m, forming a 4 x 4 grid with 2 m nodes interval. The positioning method is based on capturing the RSSI dynamics of the reflected signals, which change due to object movement below the deployed network. To reduce the influence of noise, a dynamic threshold is introduced. The links that experience a change in RSSI dynamics and exceed the dynamic threshold are called influential links. The position estimation is evaluated using three different algorithms, i.e. midpoint algorithm, intersection algorithm, and best-cover algorithm. The midpoint algorithm estimates the position as the weighted average from the midpoints of influential links. The intersection algorithm estimates the position as the weighted average of the influential links intersection points. In the best-cover algorithm, each influential link is described as a rectangular area in which the object is most likely to be found when the RSSI dynamics changes. The position estimate is derived as the area where occurrence of influential rectangles is most frequent. The best-cover algorithm outperformed the other two algorithms, with an average tracking error of 0.99 m. However, the latency of the system was around 3 seconds, making it impossible to accurately track a moving person in real-time.

The same approach adopted in (Zhang *et al*., 2007) is further developed in Zhang *et al*. (2009) to create a system capable of tracking multiple people simultaneously moving in the monitored area. In it, the nodes detecting a significant change in their RSSI values autonomously organize into clusters. The cluster head first gathers the RSSI values collected by the members of its cluster, then computes the probability of detection of an object, and finally transmits this value back to the sink node. In this way the amount of data transmitted to the base station was reduced. However, due to the cluster formation overhead and the inter-cluster communication burden, the reported latency of the system was 2 s, while the accuracy was 0.85 m for tracking one person and 1.08 m for tracking two people.

In all these studies, the power consumption of the nodes is not taken into consideration, since their radio is constantly kept on during operation. Also, the tracking relies on a previous calibration of the system, increasing its deployment time. Besides, the long-term usability of such RSSI-model based systems would also suffer from the fact that marginal changes of the conditions of the monitored indoor environment (e.g. furniture placement) can dramatically modify the propagation of radio signals and thus the RSSI values collected by the nodes, ultimately leading to the need of retraining the model.

The transmission of all the raw RSSI measurements collected by the nodes to a central base station for off-line data analysis, though effective, is not power efficient, since radio transmissions and receptions are the most power-hungry operations performed by the nodes. Also, this approach considerably increases the latency of the system, especially in multi-hop networks. These facts restrict the applicability and utility of these systems in those emergency situations such as fires, sieges, or terrorist attacks, when real-timeliness becomes a critical requirement.

At the time, the described systems are simple single-hop star networks. Large deployments capable of covering the inside of an entire building have not been proposed yet. This thesis also concentrates on a single-hop star network, but its architecture considers the requirements of an eventual large scale deployment and tackles the drawbacks and limitations experienced by other tracking systems.

2.8 Summary

The previous subsections have presented first, different wireless communication standards, protocols and briefly the uncertain nature of the wireless medium. Secondly, design factors related to WSNs were discussed since they can impact heavily the performance of the realization. Third, the related work was presented.

Wireless sensor networks operating in the 2.4 GHz ISM-band represent a suitable technology for device-free localization and tracking, since a person causes attenuation to a links radio signal when moving in the close proximity of the nodes. Since in this case additional sensors such as cameras or infrareds are not used, every deployed network could also be used to track changes in the environment. One can deploy a wireless network solely for DFL and tracking purposes or have it as an additive feature. For example in a dynamic environment, an object moving in between a link can cause temporary communication failure forcing retransmission or rerouting. If changes in the environment could be tracked in real-time, rerouting could already be performed before the route is broken, leading to superior performance.

Nowadays, DFL and tracking of people in indoor environments could potentially be exploited in a variety of applications, such as tracking of customers in shopping malls with the aim to analyze their reaction to products and advertisements placement, detection of intruders in critical buildings or infrastructures, localization of e.g. besiegers and hostages during sieges and of civilians during fires, and to enhance workers safety in industrial halls with e.g. moving machineries.

3 Experimental methodology

The following chapter starts by introducing the key components of the wireless sensor networking platform used in the developed application. The chapter continues with a thorough description of the exploited TS protocol forming the backbone of the applications communication procedure. After the radio channel characteristics in the 2.4 GHz frequency band are explained in section 3.3, the chapter ends with an overview of the characterization and variability of the RSSI measurements.

3.1 Sensor networking platform

In the following sections the sensor networking platform used in the developed application is introduced. Its radio module and MCU are presented more closely since they are central to the work done in this thesis. The RSSI measure provided by the radio module is also analyzed more closely since it represents the basis of the entire work.

3.1.1 Micro.2420 wireless sensor networking platform

The sensor networking platform used in the application, shown in Figure 4, is the U100 Micro.2420 developed by Sensinode (Sensinode, 2006). The core of the platform is a TI MSP430F1611 MCU (MSP430, 2010), having 10 kB of RAM, 48 kB of program memory, and 256 kB of flash memory. The logical clock of the MCU runs at 8 MHz. This clock is

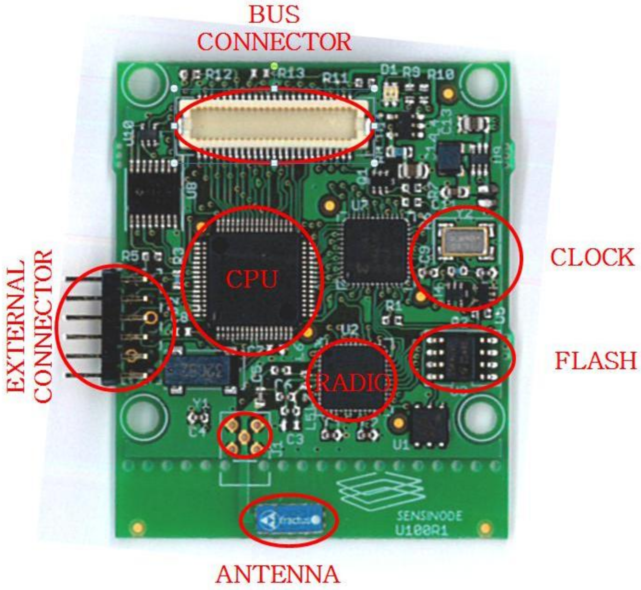


Figure 4: U100 Micro.2420 sensor networking platform (Cosar, 2009)

derived from an external 16 MHz crystal oscillator, which has an accuracy of ±40 parts-per-million (ppm). The MCU provides one 12 bit analog-to-digital converter (ADC), with up to 8 channels simultaneously, each having a voltage range of 0-3.3 V, and two 12 bit digital-to-analog converters (DACs) with a voltage range of 0-2.5 V. The radio module is a ZigBee, IEEE 802.15.4 compatible, Chipcon CC2420 transceiver (CC2420, 2010), operating in the 2.4 GHz ISM band, having a theoretical 250 kbps bandwidth. The platform runs the FreeRTOS real-time kernel (FreeRTOS, 2010) and NanoStack v1.0.3 (Sensinode, 2007), a flexible 6LoWPAN protocol stack that implements the layers of the communication stack. The dimensions of the wireless networking platform are 40 x 50 mm and it is powered by two AA batteries. The sensor networking platforms are equipped with an external omnidirectional antenna providing a 5.0 dBi gain.

3.1.2 CC2420

The CC2420 radio transceiver is designed for low power and low voltage wireless communications. The radio module provides extensive hardware support for packet handling, data buffering, burst transmissions, data encryption, data authentication, CCA, link quality indication (LQI) and packet timing information and these features reduce the load of the host MCU i.e. the TI MSP430F1611.

The RF transceiver operates in the 2400-2483.5 MHz frequency range, and it utilizes DSSS for spreading and offset quadrature phase-shift keying (O-QPSK) for modulation. Power consumption of the radio module is very low (receiving mode: 18.8 mA, transmitting mode: 17.4 mA) and it has high sensitivity (down to -95 dBm). Some key features of the CC2420 are programmable output power and channel selection in 5 MHz steps, LQI, and RSSI. (CC2420, 2010)

3.1.2.1 RSSI

The IEEE 802.15.4 physical layer provides an estimate of the power of a signal received within an IEEE 802.15.4 channel (IEEE 802.15.4, 2010). This measurement, called RSSI, is an 8 bit integer value. In accordance with the IEEE 802.15.4 standard, the RSSI value is calculated as the average received power over an 8 symbol period (128 µs). The receiver has to be enabled for at least 8 symbol periods (128 µs) for the measure to be valid, and the validity is indicated with a status bit called `RSSI_VALID`. The 8 bit RSSI measurement in dBm is stored in a register of the radio module called `RSSI.RSSI_VAL` and the value is computed as follows:

$$P_{dBm} = \mathtt{RSSI\_VAL} + \mathtt{RSSI\_OFFSET} \quad [\text{dBm}], \tag{3}$$

where `RSSI_OFFSET` is an experimental constant (approximately -45 dBm) derived during the radio module development. The dynamic range of the RSSI is approximately 100 dBm, from -100 dBm to 0 dBm. The RSSI values measured by the CC2420 transceiver behave in a linear fashion, but the radio module includes also multiple nonlinear regions (Chen and Terzis, 2010). The RSSI measure provided by the transceiver has a ±6 dB accuracy of the actual received signal strength value. (CC2420, 2010)

3.1.3 TI MSP430 MCU

The MSP430F1611 MCU by Texas Instruments is specially designed for low cost and low power applications such as embedded systems and it is well suited for battery-powered RF devices. The MCU is based on a 16-bit RISC processor that uses a von Neumann architecture that shares the single address space among the peripherals, RAM, and Flash/ROM memory. The central processing unit (CPU) incorporates 16 16-bit registers, of which four (R0-R3) are dedicated to special functions, and the rest are available for general use. The microcontroller does not have an external memory bus and so is limited to on-chip memory (256 KB of flash memory and 10 KB of RAM)

The flexible clock system of the MCU is designed for low power applications. The clock system consists of a low-frequency auxiliary clock (ACKL) and a master clock (MCKL) which is derived from an integrated high-speed digitally controlled oscillator (DCO). The ACKL enables ultralow-power stand-by mode, whereas the MCKL is used by the CPU and the high-speed peripherals assuring high speed signal processing. For reducing power consumption even further, the MCU provides six different operating modes that account for three different needs: ultralow-power operation, speed and data throughput and minimizing the power consumption of individual peripherals. The power modes enable turning off the unused clocks of the MCU’s clock system and disabling the power hungry CPU. In idle mode (all clocks and the CPU disabled) the current consumption of the MCU is 0.1 µA. The MCU also has two 16 bit timers/counters, called Timer-A and Timer-B. Timer-B is used to maintain the nodes local clock for task scheduling and MAC layer operations, while Timer-A is software-configurable. (MSP430, 2010)

3.2 Time synchronization

The Sensinode Micro.2420 sensor networking platform is equipped with a low-quality oscillator (±40 ppm) which introduces a significant clock drift (node A has the highest skew, equal to 3.83 µs/s in Figure 5). In addition, the drift is different in each node, as shown in Figure 5, which illustrates the drifts of five different nodes. The clock drift depends also on the nodes age and operating temperature. Therefore in applications relying on e.g. very accurate sampling or communication intervals, it becomes essential to accurately synchronize the nodes, not only at the beginning, but also throughout the whole execution of the application.

The application developed in this thesis exploits a MAC layer time synchronization protocol, named µ-Sync, originally introduced by Mahmood and Jäntti (2009). This protocol, deriving from the flooding time synchronization protocol (FTSP) (Maróti *et al.*, 2004), was initially implemented on a different hardware, i.e. TI CC2431 (CC2431, 2010), and it has recently been ported to the Micro.2420 platform (Bocca *et al.*, 2011).

3.2.1 µ-Sync protocol framework

The accuracy of TS is affected by issues such as the unreliability's of the wireless medium as well as from implementation and hardware aspects. In the communication stack executed by the nodes, forwarding radio packets among layers consumes a considerable amount of time (e.g. 3.8 ms on average from the application layer to the MAC layer). Most importantly, this forwarding time contains jitter. This fact plays against accurate TS, which relies on a fixed communication time in the critical path between sender and receiver. By time-

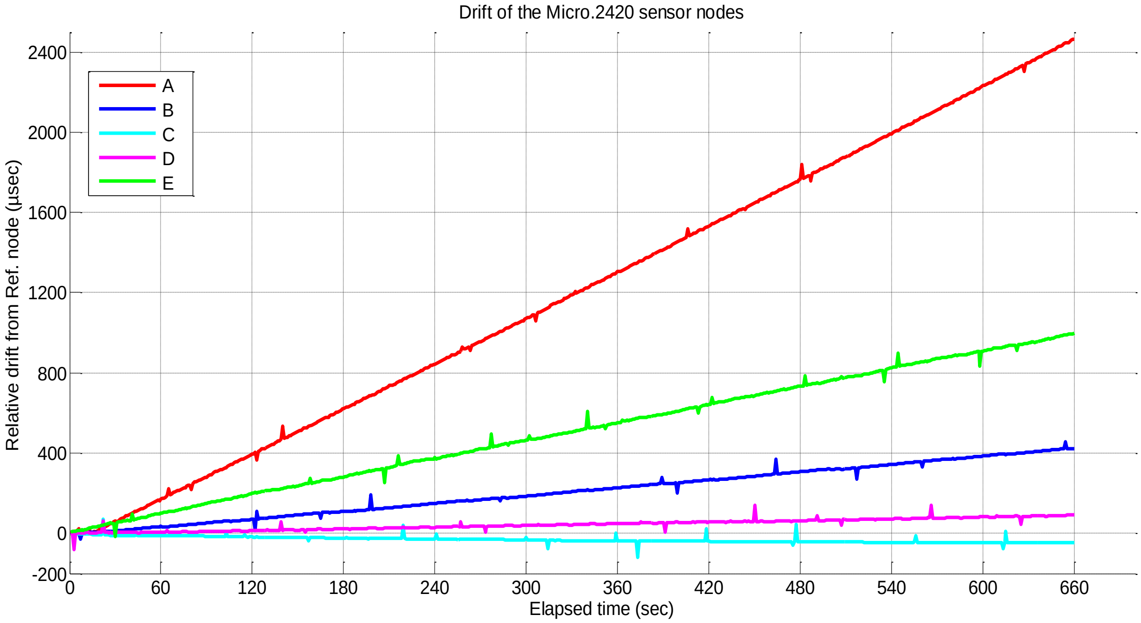


Figure 5: Clock drift of five different Micro.2420 sensor nodes (Bocca *et al.*, 2011) It is to be noted that the clocks deviate in both positive and negative direction with respect to the reference clock. Drift of node C is the lowest, whereas node A experiences a drift of 3.83 µs/s which accounts for the highest skew of the five nodes. In other studies, some nodes have been reported having a clock drift in the magnitude of 16 µs/s, which is an astonishing 1 ms/min.

stamping the synchronization packets at the lowest layer possible (MAC layer), jitter and the time between transmission and reception are minimized. As a result, the *μ-Sync* protocol achieves accuracy in the order of microseconds.

3.2.2 Implementation

Of the two clocks provided by the MCU of the Micro.2420 platform, Timer-A is free and thus can be exploited for TS. This timer has one 16-bit timer/counter (TAR) and three 16 bit configurable compare/control registers (TACCRx). The 8 MHz clock source provided by the MCU is divided by 8 before being passed to Timer-A, resulting in a tick resolution of:

$$t_{tick}=1/f_{nominal}=1\mu s. \tag{4}$$

The value of TAR increases at every tick of the clock, starting from 0, up to its maximum value of 2^{16}-1 = 65535. Once the maximum value has been reached, the timer overflows generating an interrupt. Therefore, since the tick resolution equals 1 μs, an *overflow* interrupt is generated every:

$$T_{overflow} = t_{tick} \cdot \left(2^{16} - 1\right) = 65.535 \text{ ms.} \tag{5}$$

Furthermore, each *overflow* interrupt increments a 32-bit logical clock counter, named $N_{logical\text{-}clock}$. The inaccuracy of the clock of the nodes is caused by the variations of $T_{overflow}$, due to the changes in the crystal oscillator nominal frequency, which in turn is due to its low quality, aging, operating temperature, etc.

In the developed application, all the nodes of the network are time synchronized with the clock of the sink node, which represents the global time of the network. The local time of the sink node (t_{local}) is broadcasted to all the other nodes in a *sync beacon* packet, containing both the current value of TAR and $N_{logical\text{-}clock}$. With these two values, the local time of the sink node can be computed as:

$$t_{local} = \left(N_{logical-clock} \cdot T_{overflow}\right) + \left(TAR \cdot t_{tick}\right). \tag{6}$$

Since the interrupts triggered by $T_{overflow}$ are generated by the *overflow* period, it cannot be used for triggering events below 65.535 ms. However, it is not uncommon that the nodes of a sensor network are sampling or communicating at a higher frequency than the one set by $T_{overflow}$. Timer-A provides three 16-bit configurable compare/control registers which can be used to generate interrupts at a higher frequency. In the developed application, the desired interrupt frequency is set by assigning to the TACCR1 register the time interval Δ*t* between the interrupts. Each time a Δ*t* interval expires, an interrupt is generated. In its interrupt service routine (ISR), TACCR1 is updated by adding to its current value the defined time interval Δ*t*, and an I/O pin of the Micro.2420 node is toggled. The toggling of the pin is observable at every layer of the stack, and it represents the "heart beat" of the application.

As a result of the execution of the TS protocol, the nodes of the network, assuming they have received the *sync beacons* broadcasted by the sink node, generate synchronous interrupts. In this way the nodes can be set to sample simultaneously, or to communicate in a TDMA fashion.

3.2.3 Clock skew

The low-quality crystal oscillator found in the Micro.2420 nodes introduces relative clock skew among the nodes, i.e. deviation from reference time that is unique for each node. The transmission of *sync beacons* by the sink node compensates the initial clock offset of the nodes. Since the initial clock offset is compensated upon the first *sync beacon,* the clocks of the sink and the nodes correspond to one another. However, after the initial synchronization process, the clocks of the nodes start deviating at different speeds from each other again, as shown in Figure 5, due to the relative clock skew. To avoid this problem the nodes also estimate their clock drift with respect to the sink during the synchronization period. At the beginning of the synchronization phase, the sink node transmits a predefined number of *sync beacons* at regular intervals. At the reception of a *sync beacon*, the receiving nodes estimate their own clock drift and adjust their clock to match to the one of the sink node. The obtained drift estimates are saved in an array which is then used to compute the median for the relative clock drift value, which is finally used to periodically readjust the clock. In this way, the nodes are able to autonomously keep themselves synchronized over long periods of time without the transmission of additional *sync beacons* from the sink node.

3.2.4 With time synchronization towards accurate TDMA

In the application developed in this thesis, the communication follows a slotted TDMA scheme. In each slot only one node broadcasts a packet while the rest of the nodes listen to the broadcast. At the next slot, the role of the transmitter is passed to the next node. In WSNs applications, a common way of passing the transmitter role around is a token passing protocol, in which each node is assigned an ID number and programmed with a known order of transmission. Upon packet reception, each node examines the transmitter's identification number to check if it is their turn to transmit next, and if not, they wait for the next node to transmit. This procedure is vulnerable to packet drops, since the transmission turn is assigned based on the received packets. Token passing protocols are also especially hard to handle when transmission frequencies are high due to clock skew and critical path jitter between the sender and receiver. Accurate time synchronization of the network detaches the node dependences, since transmission and reception slots are determined locally in the nodes based on the interrupts as explained in 3.2.2.

In the developed application after TS is performed, each node is assigned slots for transmission and reception in a TDMA fashion. In the application, the transmission slots are assigned based on the unique ID number of the nodes. All the other slots are reserved for receiving packets broadcasted by other nodes. Thanks to the accurate time synchronization, the nodes know the transmission times of the other nodes, and because of this, they can turn off the radio for the times that receptions are not expected, thus saving energy.

3.3 Radio channel characteristics of the 2.4 GHz frequency band

In recent years, the 2.4 GHz ISM band has become particularly popular among wireless systems. This frequency band is shared among several coexisting standards which can interfere one another. Possible sources of interference for IEEE 802.15.4 are IEEE 802.11, Bluetooth, microwave ovens, etc (ZigBee, 2010). In the following sections, the overlapping frequency spectrums of IEEE 802.11b and IEEE 802.15.4 standards are described and interference of IEEE 802.11b to IEEE 802.15.4 is analyzed. To maximize the performance of the WSN, an interference free channel was found and used during later tests.

3.3.1 IEEE 802.11b and IEEE 802.15.4 frequency spectrums

The IEEE 802.11b and IEEE 802.15.4 standards both operate in the unlicensed ISM frequency band where bandwidth allocation is not guaranteed. The IEEE 802.15.4 divides the 2.4 GHz band into 16 channels having a bandwidth of 2 MHz each and the channels are separated by intervals of 5 MHz. Correspondingly, the IEEE 802.11b divides the frequency spectrum into 13 channels having a bandwidth of 22 MHz each and spaced only 5 MHz apart. Since the channels of the two standards are overlapping, only few channels of IEEE 802.15.4 are interference free. Figure 6 illustrates the frequency spectrums of IEEE 802.11b and IEEE 802.15.4. According to Figure 6, channels 15, 20, 25 and 26 of IEEE 802.15.4 do not overlap with the channels used in IEEE 802.11b.

Because of the shared frequency band, it is plausible that coexisting systems can interfere, as demonstrated in Srinivasan *et al.*, (2006a), where the interference of IEEE 802.11b to IEEE 802.15.4 was revealed. In the experiments, time synchronized nodes were used in order to measure the spatial correlation of the noise sensed by the nodes. The high correlation between the nodes confirmed its external origin. To prove that the noise was generated by the coexisting IEEE 802.11b network, the measurements were collected with and

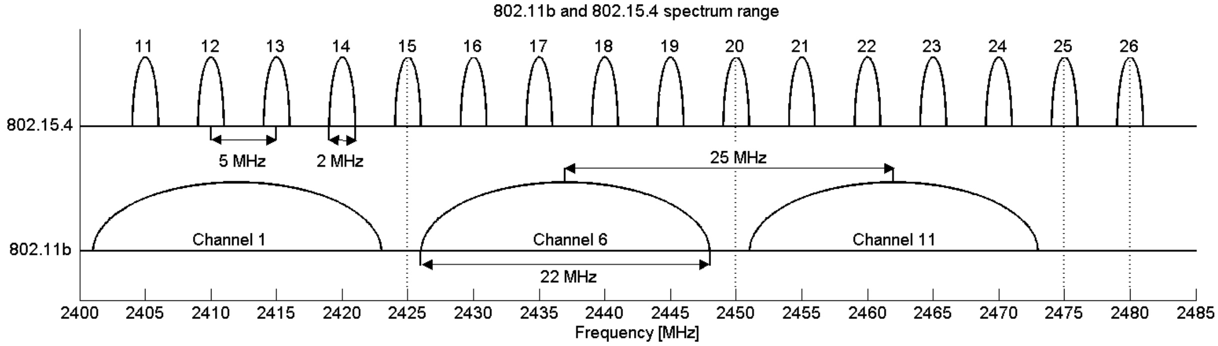


Figure 6: Channel spectrum of IEEE 802.11b and IEEE 802.15.4

without shielding the nearby IEEE 802.11b access points. The conclusion was that the noise was generated by the WLAN, and also that the packet losses in the IEEE 802.15.4 network are highly correlated over short time periods, but are independent over longer periods of time.

3.3.2 Interference of coexisting systems

In the previous section the frequency spectrums of IEEE 802.11b and IEEE 802.15.4 were presented. This section shows how the interference of 802.11b affects the performance of IEEE 802.15.4. Tests were made as in (Srinivasan *et al.*, 2006b). Four time synchronized nodes were deployed in different locations of an indoor environment to measure the spatial correlation of noise generated by WLAN. All 16 IEEE 802.15.4 channels were scanned in order to evaluate the noise in each channel. Every channel was scanned for 200 ms at a rate of 1 kHz. The measurements were stored in the external flash memory of the Micro.2420 platform for offline analysis. Figure 7 illustrates on the left the noise sensed by the four nodes on channel 12, which overlaps with channel 1 of IEEE 802.11b. On the right, the measurements on channel 26 are shown which does not overlap with IEEE 802.11b channels.

None of the nodes sense noise on channel 26, while on channel 12 all the nodes sense a consistent noise. The correlation of the noise sensed by the four nodes on channel 12 is:

$$r_{XY} = \begin{bmatrix} 1.00 & 0.96 & 0.95 & 0.95 \\ 0.96 & 1.00 & 0.96 & 0.97 \\ 0.95 & 0.96 & 1.00 & 0.96 \\ 0.95 & 0.97 & 0.96 & 1.00 \end{bmatrix}$$

confirming the hypothesis that the noise is generated by an external source. Some of the consequences of the interference generated by WLAN are discussed in the following.

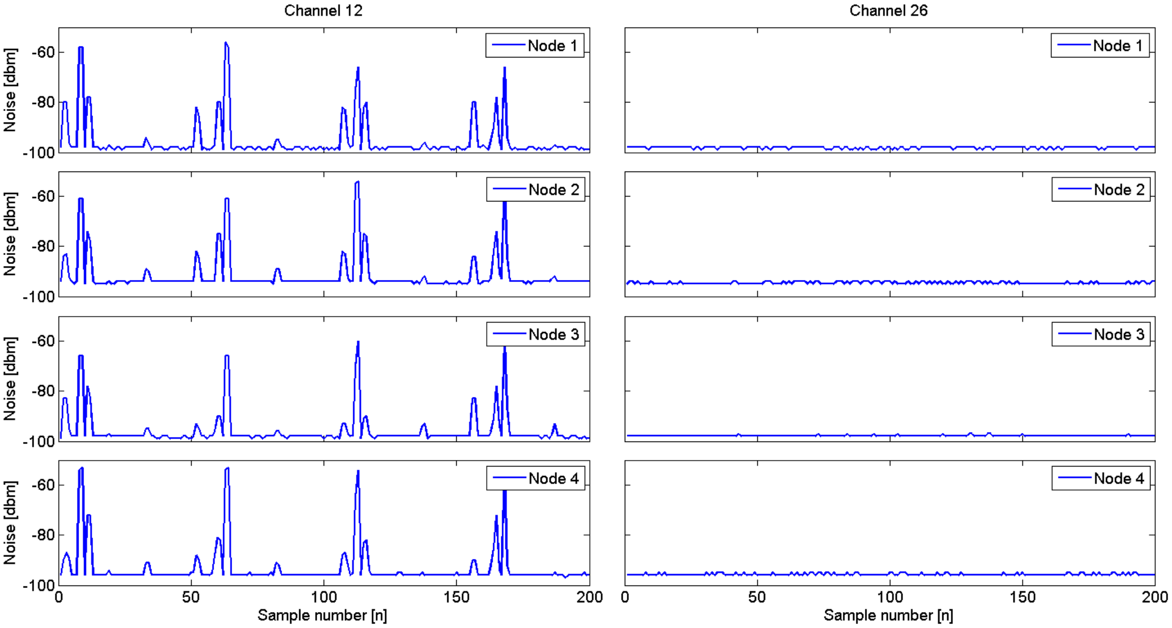


Figure 7: Noise of channel 12 on the left, and channel 26 on the right. Channel 12 of IEEE 802.15.4 operates on the same frequency range as channel 1 of IEEE 802.11b.

In Sikora *et al*. (2005) it was shown that, in the worst case scenario, approximately 90 % of all WPAN-frames were destroyed by the interference of WLAN when overlapping channels were used. Also, the work proved that when non-overlapping channels were adequately chosen, the influence of WLAN on IEEE 802.15.4 cannot be observed. The work in (Petrova *et al*., 2006) showed that an offset of at least 7 MHz has to exist between the operational frequencies of IEEE 802.15.4 and IEEE 802.11b/g for a satisfactory performance of the IEEE 802.15.4 network. The results also indicated that the frame error rate (FER) increased as a function of packet size, i.e. packets with a small payload coped with interference better. The effect of node distance was studied by Shuaib *et al.* (2006). They concluded that the throughput of IEEE 802.15.4 decreased by 14 % when the node interval was raised from 6 to 12 meters in a noisy environment.

The interference may have a major influence on the performance of the system and the coexistence of WLAN has to be considered when deploying a WSN. A suitable channel could be chosen from the channels that do not overlap with the channels of WLAN. However, it cannot be guaranteed that these channels are not affected by other external interference sources. In order to find the best plausible channel to be used during later tests, the channels of the whole frequency spectrum have to be ranked. In the following section, two simple yet effective methods to rank radio channels are introduced.

3.3.3 Ranking of the radio channels

A radio channel characterized by low WLAN interference can significantly improve the performance of the network and add reliability of communication. In the following, WLAN interference on the 16 IEEE 802.15.4 channels are analyzed, and the channels are ranked using different criteria, i.e. cardinality and the Goertzel algorithm.

Cardinality describes the number of different elements in a set. In this case, the cardinality describes how many different RSSI values, i.e. noise values, are observed during the 200 ms sampling window. A large number of values indicate a noisy channel, whereas a low number of values refers to a channel with low interference.

The Goertzel algorithm is a digital signal processing technique for identifying specific frequency components of a signal. The algorithm is a disguised discrete Fourier transform (DFT) that computes the k^{th} DFT coefficient of the input sequence $x[n]$ using a second-order filter as follows:

$$s_k[n] = x[n] + 2\cos\left(\tfrac{2\pi k}{N}\right) s_k[n-1] - s_k[n-2], \tag{7}$$

where N is the total number of samples and $s[-1] = s[-2] = 0$ (Shaterian and Gharaee, 2010). The corresponding power of the k^{th} coefficient can be calculated as follows:

$$\left|X[k]\right|^2 = s_k^2[N] + s_k^2[N-1] - 2\cos\left(\tfrac{2\pi k}{N}\right) s_k^2[N] s_k^2[N-1]. \tag{8}$$

The magnitude of the frequency spectrum in the considered frequencies of interest is computed by taking the square root from the corresponding power expressed in (8). The algorithm can be iteratively executed during the sampling and coefficient $2\cos\left(\tfrac{2\pi k}{N}\right)$ can be computed before hand, leading to light calculation during run time. The algorithm is implementable to real WSN applications without using all the resources of the MCU.

The noise measurements gathered in section 3.3.2 are analyzed and the radio channels are ranked. Figure 8 illustrates four channels, i.e. channels 12, 15, 17, and 26, that are ranked using the cardinality criterion and the Goertzel algorithm. Two of the four considered channels, i.e. channels 12 and 17, overlap with IEEE 802.11b, while the other two considered channels, i.e. 15 and 26, do not overlap with the WLAN channels. The results imply that those IEEE 802.15.4 channels that overlap with the channels of IEEE 802.11b should be avoided in order to maximize the performance of the network. During later tests channel 26 is used to guarantee favorable conditions for communication.

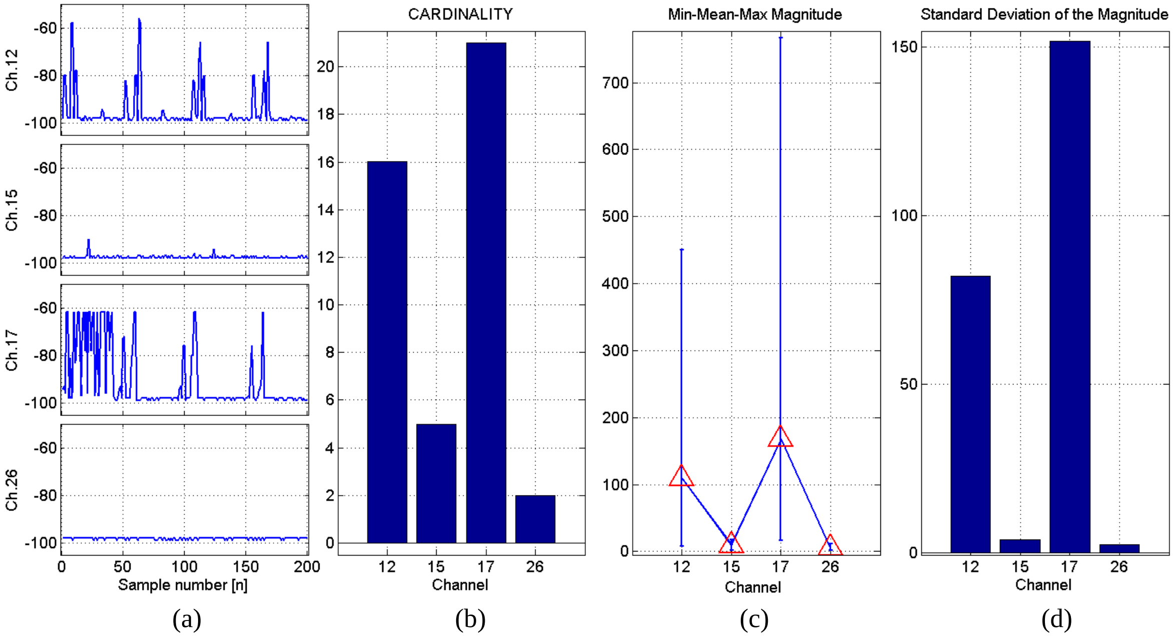


Figure 8: Ranking 4 radio channels of IEEE 802.15.4. The interference of 802.11b on each channel is shown in inset (a). Overlapping channels (12 and 17) contain interference, whereas the two non-overlapping channels (15 and 26) do not. The cardinality criterion is illustrated in inset (b), and it ranks the channels as 17 being the worst and 26 the best. Mean, maximum, and minimum values of the frequency spectrum magnitude obtained with the Goertzel algorithm are shown in inset (c) and the standard deviation of the frequency spectrum magnitude in inset (d). The statistical values of the Goertzel algorithm also rank channel 17 as the noisiest channel while 26 being the most interference free.

3.4 Characterization of radio signal strength variability

Three distinct factors affect the received radio signal strength: distance of the communication pair, transmission power, and the surrounding environment. In the following sections, the effects of these factors are analyzed, and the characteristics of the RSSI are presented in detail. The characterization starts by investigating the influence of the transmission power, and is followed by an analysis of the effect of distance on the RSSI. The influence of distance is studied in three different environments, and a log-normal signal propagation model is derived for each environment. At the end of the section, the derived models and the collected test results are compared. The RSSI behavior in different environments is discussed in section 3.4.3 together with the causes of RSSI variability.

3.4.1 Transmission power

The Chipcon CC2420 radio module defines eight different output power levels (CC2420, 2010), ranging from -25 dBm to 0 dBm. The output power can be selected at the application layer of NanoStack as a percentage value from 0 to 100 %, where 100 % corresponds to 0 dBm and ~10% corresponds to the minimal output power of -25 dBm. The expected strength of the radio signal with given transmission power in dBm is given by:

$$P(d) = P_T - P_{ref}(d_0) \tag{9}$$

where P_T is the transmission power (-25-0 dBm) and P_{ref} (d_o) is the reference output power measured at distance d_o. To study the relation between the measured RSSI values and the output power levels reported in (CC2420, 2010), a test was conducted using four nodes communicating in a TDMA fashion. The output power of the nodes was decreased from 100 % to 10 % in steps of 10 % and at each power level every node broadcasted 300 packets. The nodes were placed along a line in 1 m intervals.

Figure 9 illustrates the measured RSSI values (solid line) and the expected signal strength (dashed line). The expected signal strength is given by (9), where P_{ref} (d_o) is substituted with the maximum output power at distance ($d_o \in \{1, 2, 3\text{ m}\}$) and the results are shown in Table 3.

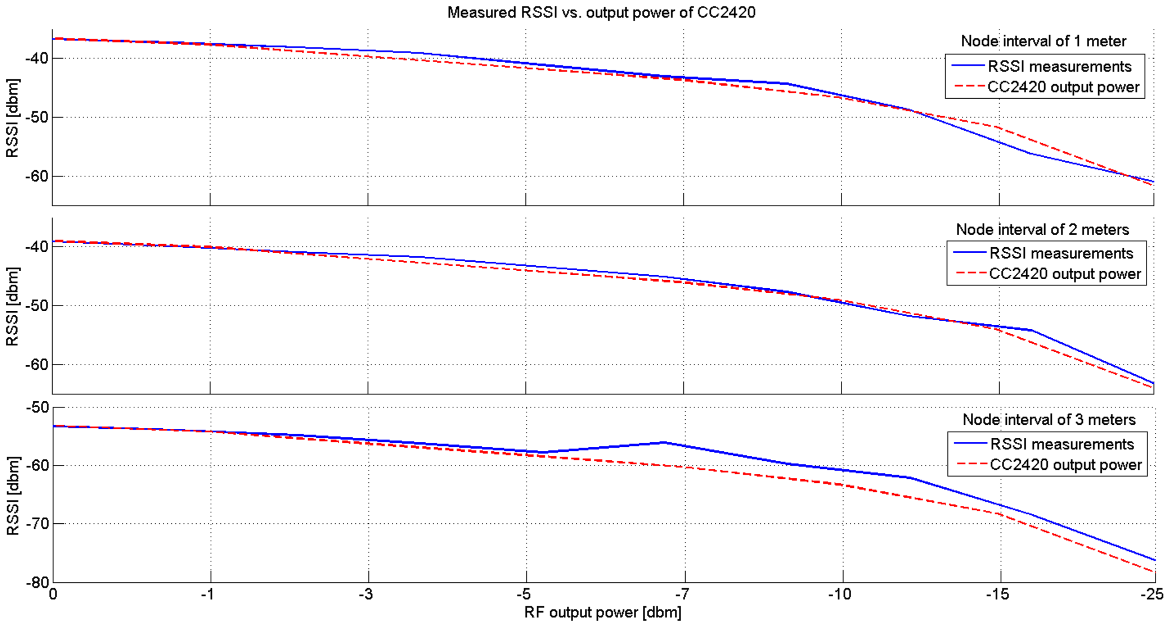


Figure 9: Measured RSSI values as a function of output power shown with solid line. Expected output power levels given in (CC2420, 2010) illustrated with dashed line.

Table 3: Reference output power measured at different distances.

d_o [m]	1	2	3
P_{ref} [dBm]	-36.6	-39.0	-53.3

The measured RSSI values match the expected signal strength at high output power levels, but show deviation at lower output power levels. All measurements show a nonlinear region when the received signal strength is between -50 and -60 dBm. In (Chen and Terzis, 2010), the same nonlinearities of the RSSI measurements were observed (tests conducted with Tmote Sky motes equipped with CC2420 radio modules). The results imply that RSSI behavior is mostly linear, apart from multiple nonlinear regions. Since the nonlinearities existed for all the nodes that were tested in the work, the conclusion was that the systematic errors in the RSSI measurements were introduced by the CC2420 radio.

3.4.2 Distance

The results listed in the previous section demonstrated that the RSSI measurements collected at a given position decreased as the output power was reduced. The impact of distance can already be observed from Figure 9, where the nodes located further away collected lower RSSI measurements. However, the test setup was not adequate to study the effect of distance on the RSSI, because the tested nodes distances were rather small. In the following, the influence of distance on the RSSI is studied in three different environments:

- The 1st environment is the lobby of TUAS-building which is an open indoor environment. The measurements are gathered at intervals of 1 meter from 1 to 40 meters. After 10 meters the lobby narrows down in to a spacious corridor.
- The second habitat is the corridor of Control Engineering laboratory located on the 3rd floor of TUAS-building. The corridors size is 1.6·2.5 m ($w{\cdot}h$) and it is considerably smaller then the corridor of the lobby.
- The last environment is a parking lot, which replicates a free area where no obstacles or reflecting surfaces are present, in the close neighborhood of the testbed.

The test was conducted using two nodes communicating in a TDMA fashion with a 32 ms cycle time. During a cycle, each node transmitted and received one packet. The sequential number of the packets and the corresponding RSSI measurements were stored in the external flash memory of the Micro.2420 platform for off-line analysis. The average RSSI measurements and the packet reception rate (PRR) were evaluated from a set of 150 measurements at each location. Radio signal attenuation and PRR in the three environments are shown in Figure 10.

The RSSI behavior is non-consistent over small changes in the distance, but in general it decreases as a function of distance. The observed signal strength is higher at most distances in the corridor setup then in the lobby or parking lot. The corridor acts as a waveguide (Mottola *et al.*, 2010), in which the radio signals bounce along the corridor walls. In the

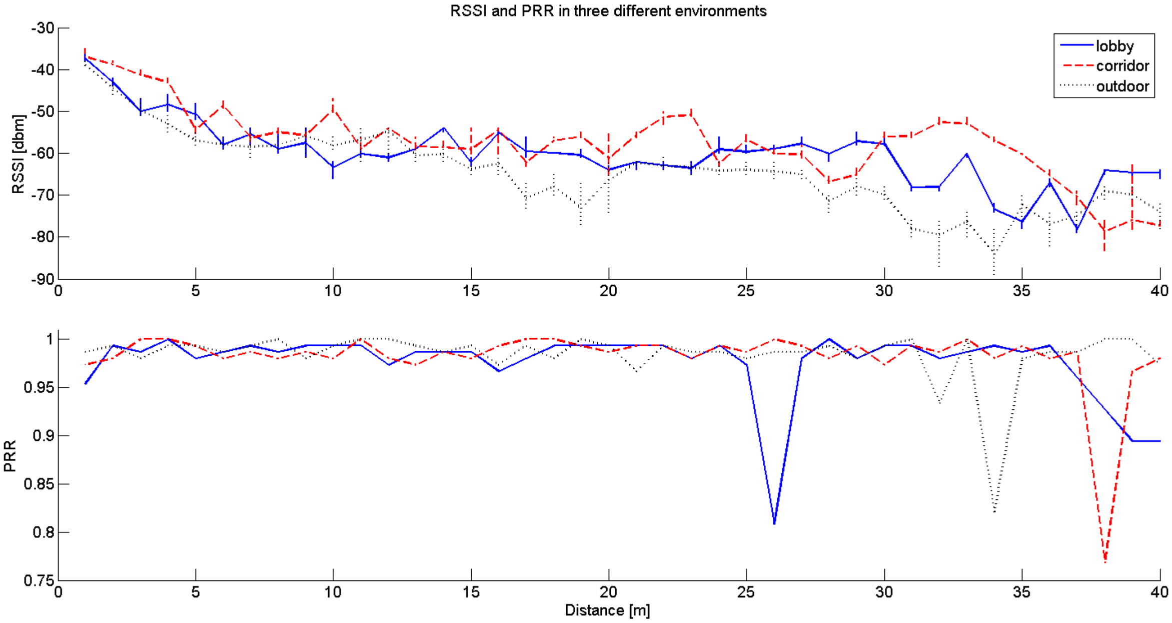


Figure 10: Measured RSSI values as a function of distance in three different environments illustrated above and the PRR of each measurement set below. The used output power was 0 dBm.

outdoor environment, where the attenuation is faster, the radio waves propagate in all directions, contrary to the corridor and lobby.

The PRR remains high in all environments at most distances. However, in each studied environment, one or more drops of the PRR are observable. Zhao and Govindan, (2003) also identified that PRR depends on the spatial position of the nodes. In their work, packet loss was studied in different habitats, and large variation in PRR was revealed for nodes located in the gray region (area where communication cannot be assured). Moreover, the gray regions size and distance from the transmitting node was different in each environment. Figure 10 reveals that in the corridor and parking lot environments, the RSSI magnitude decreases considerably in the preceding measurement positions before an evident drop in the PRR occurs. For example, the decrease of the RSSI over a 5 meters distance is -25 dBm for the corridor and -15 dBm for the parking lot.

In the three studied environments, the LoS path between the communicating nodes was unobstructed. If the nodes were communicating e.g. through walls or other obstacles, it could be expected that the attenuation would be even stronger and in that case the communication distances would be lower.

3.4.2.1 Path loss prediction model

A commonly used signal propagation model is the log-normal shadowing model:

$$P(d) = P_T - P_{ref}(d_0) - 10\eta \log_{10}\left(d / d_0\right) + X_\sigma \tag{10}$$

where P_T is the transmission power (0 dBm), P_{ref} (d_o) is the signal strength at reference distance d_o, η is the path loss exponent, and X_σ is a Gaussian random variable with zero mean and σ^2 variance (Rappaport 1996). In the following the path loss model is derived for each environment introduced in section 3.4.2. The signal strength P_{ref} (d_o) is substituted with the measured signal strength at the reference distance of 1 m. The path loss exponent is derived by minimizing the following cost function:

$$J_{iae} = \sum_{1}^{40} \left|e(d)\right| = \sum_{1}^{40} \left|P(d) - x(d)\right|, \tag{11}$$

where x(d) is the RSSI measurement at distance d. The results are shown in Table 4. The corridor environment has the smallest path loss exponent (1.6), while the parking lot has the highest (2.1). The results are consistent with (Rappaport 1996), where for LoS indoor environments a 1.6-1.8 coefficient is reported, and for outdoor environments a constant of 2.0. A second interesting result is represented by the values of the cost function, where the outdoor environment achieves the lowest result. In open environments, such as the lobby and the parking lot, multipath phenomenon is minimal, and the log-normal shadowing model predicts the signal behavior better then in indoor environments where multipath is present. Multipath leads to unpredictable RSSI behavior as in the corridor setup. The average error $\bar{e}$ between the model and the measurements, and the variance σ^2_{error} and standard deviation σ_{error} of the error imply the same conclusions about the effects of multipath in open and confined areas. The more open the environment is, the less the RSSI measurements deviate from the values derived by the model. A comparison between the log-normal shadowing model and the collected measurements in the three environments is presented in Figure 11.

Table 4: Environment dependent path loss exponent which minimizes the error between the measurements and the model. Calculated cost function and average, variance and standard deviation of the measurement error are shown.

	η	J_{iae}	$\bar{e}$	σ^2_{error}	σ_{error}
Lobby	1.9	140.25	3.51	8.17	2.86
Corridor	1.6	185.59	4.64	14.31	3.78
Parking lot	2.1	133.88	3.34	7.33	2.71

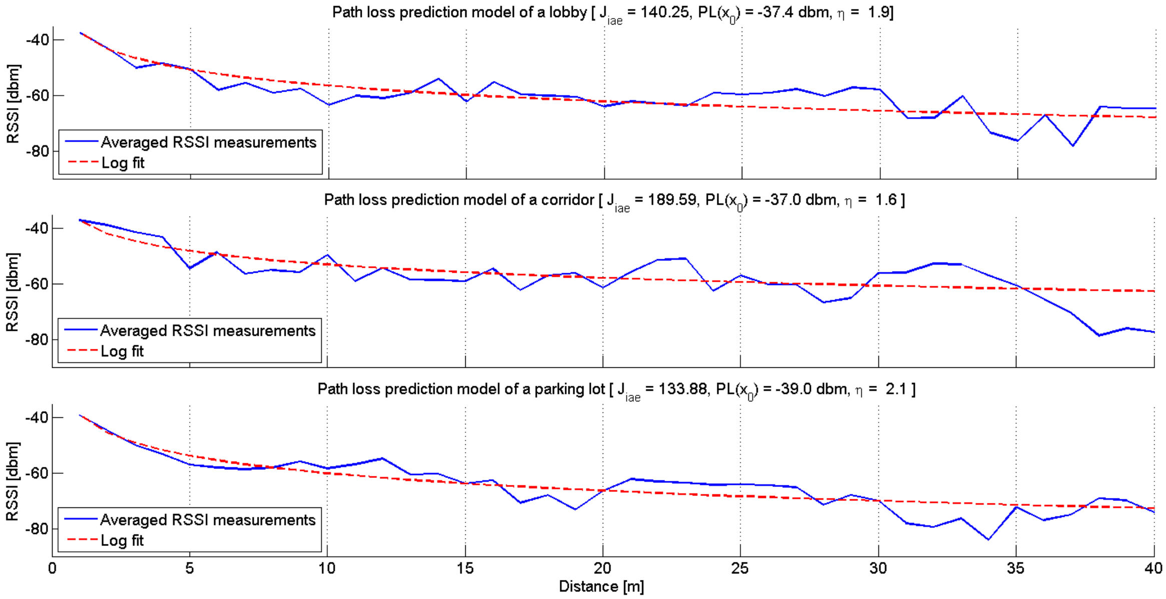


Figure 11: Comparison of log-normal shadowing signal propagation model vs. measured RSSI values in three different environments.

3.4.3 The effect of the surrounding environment

In the previous sections, the effect of distance and transmission power on the RSSI was investigated in obstacle free environments. In the following, the radiation pattern of the antenna and the effect of nodes positions are discussed. The radiation pattern of the antenna was examined by collecting RSSI measurements around a central node at intervals of 1 meter and 45°. The procedure to collect RSSI measurements was the same as described in section 3.4.2. The orientation of the central node was not changed during the measurements. To explore the effect of walls to the radiation pattern of the antenna, the measurements were also collected in a corner of a hall and in an office environment.

Figure 12 illustrates the radiation pattern of the antenna in a free environment (left side) and in an area confined by walls (right side). The central node is positioned to the origin in both experiments whereas the black dots represent the measurement positions. The radiation patterns are achieved by interpolating in between the collected measurements. In the obstacle free area, the radiation pattern is slightly asymmetrical due to the imperfect radiation pattern of the omnidirectional antenna. This result implies that the node orientation has a great impact on the RSSI measurements. For example, at a distance of 3 meters from the central node, a difference of 10 dBm is measured between the highest and lowest RSSI value, confirming the results reported in (Lymberopoulos *et al.*, 2006). In their tests, a maximum difference of 11 dBm was obtained in equivalent regions of the radiation pattern.

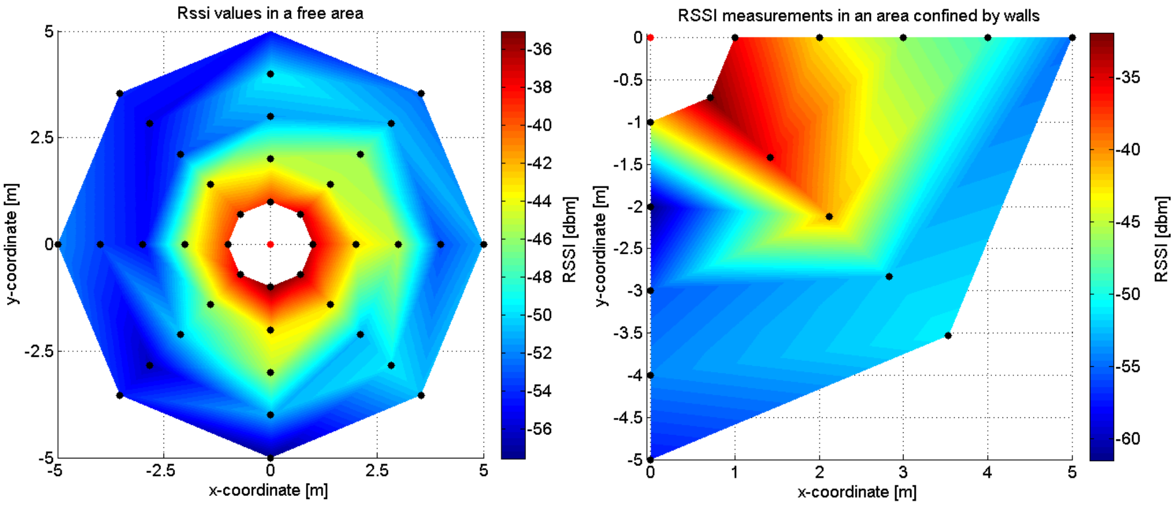


Figure 12: RSSI in a free area shown on the left and in a confined area shown on the right. RSSI values in the confined area are considerably weaker than in the free area. The irregular radiation pattern of the omnidirectional antenna can be observed from the measurements conducted in the free area.

In the confined area, walls are located on the two axes spanning from the origin. The radiation pattern along the y-axes is considerably weaker compared to the free area; a maximum difference of 18 dBm is measured at position (0, -2). On the other hand, along the x-axes, and along the direction -45^0, the RSSI values are on the average higher in comparison to the free area. On average, the RSSI measurements are 0.8 dBm higher along the x-axis in the obstructed environment. Correspondingly in the direction of -45^0 a difference of 3.6 dBm on average is recorded in favor of the corner.

Concerning the propagation of radio signals; an obstacle free space is the most beneficial environment to deploy a WSN, but it is not the most likely habitat for WSN deployment. In the real world, WSNs are most likely deployed in environments, such as offices, retail stores, and on the ground floor of industrial warehouses, where obstacles, walls, etc. exist. The radiation pattern is therefore examined in an office environment, where plaster walls, cabinets and other obstacles affect the propagation of radio signals. The positions of the nodes are shown in Figure 13, where also the walls are illustrated with thick black lines.

It is clear that in an office environment, where LoS communications are rare, attenuation is much stronger and much more irregular than in free areas. The radio signal strength does not decrease solely as a function of distance and modeling the RSSI becomes highly complex, when irregular attenuation, multipath, etc. have to be considered. It is highly unlikely that communication range can reach the distances derived in section 3.4.2. It is also to be noted that the walls in the office environment were made of light material (plaster). The

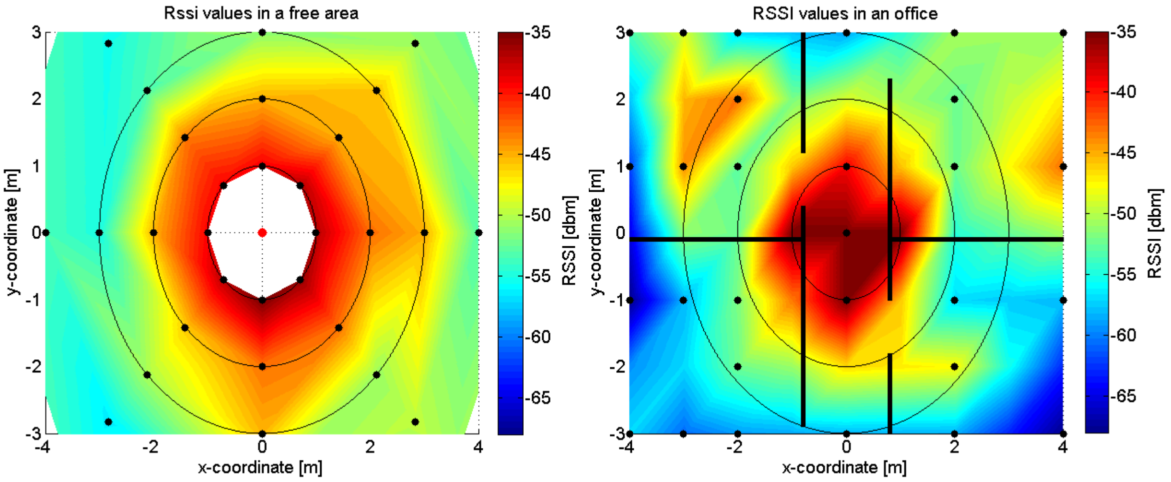


Figure 13: Comparison of the RSSI in a free area on the left and in a confined office, where walls and other obstacles disturb the propagation of the radio signal. Radiation pattern in an office is highly irregular and attenuation of the radio signal is faster than in an open environment.

attenuation could be expected to be even faster in environments where walls are made of brick or concrete.

3.4.4 Sources of RSSI variability

The sources of RSSI variability are many, e.g. multipath, fading, antenna differences, node orientation, surrounding environment, distance between communicating nodes, etc. In the previous sections, some of these issues, i.e. transmission power, node orientation, distance, and the effect of the surrounding environment, were presented and discussed. A more thorough analysis of the RSSI variability is made in Lymberopoulos *et al.,* (2006). The fact that the RSSI measure varies, denotes that the RSSI cannot be modeled accurately beforehand even though node locations would be known. In the context of this thesis, the algorithm developed to detect intrusions does not rely on hard coded thresholds because of the RSSI variability. The embedded algorithm and the intrusion detection system were developed to adjust to the variability of the RSSI measure and to react to the changes in the environment.

4 RSSI based intrusion detection

In recent years, there has been an increasing interest in utilizing RSSI for surveillance and motion tracking purposes. This measure has been found to be useful for these intentions since RSSI measurements are nearly constant in a static environment, but show increasing variance when the conditions change, e.g. when a person walks through the area.

The related work introduced in section 2.7 confirms the validity of using the RSSI for detecting people inside the monitored area. Differently than in the work conducted by others, this thesis focuses on processing the RSSI measurements locally in the nodes in real-time while the application is running. In the work done by others, RSSI measurements are analyzed externally and the nodes in the network are not aware of the intrusions. Also in some cases the measurements are post-processed after run time.

The aim of this thesis is to create a WSN capable of detecting the intrusion caused by a person, estimate the position from the aggregated data and to track the intruder in real-time inside the monitored area. The intrusion detection is performed in a distributed fashion, locally by each node, only by means of processing the RSSI measurements. The intrusions sensed by individual nodes are sent to the sink node. Situation awareness is obtained by aggregating the alerts of all nodes and tracking is performed in real-time on a computer connected to the sink node. In addition, the aim is to exploit TS to enable TDMA based communication and to turn off the radio when scheduled communications are not expected.

In this chapter an intrusion detection system is introduced and since the RSSI measurements vary unpredictably, no information can be retrieved from the magnitude of the RSSI. For example if a person would be located in the area where a new WSN is set up at the time of deployment, the RSSI would not indicate the presence of the person supposing that the person would stay still at all times.

4.1 Overview of the application

The intrusion detection application consists of three parts: network configuration, synchronization and the intrusion detection tasks. Configuration and synchronization of the sensor network are performed before the actual intrusion detection task begins. To increase the flexibility of the application, some network parameters such as the radio channel and transmission power are not hard coded to the program code, but can be set by the end user before network configuration. In the following, the configuration and synchronization procedures are described in more detail.

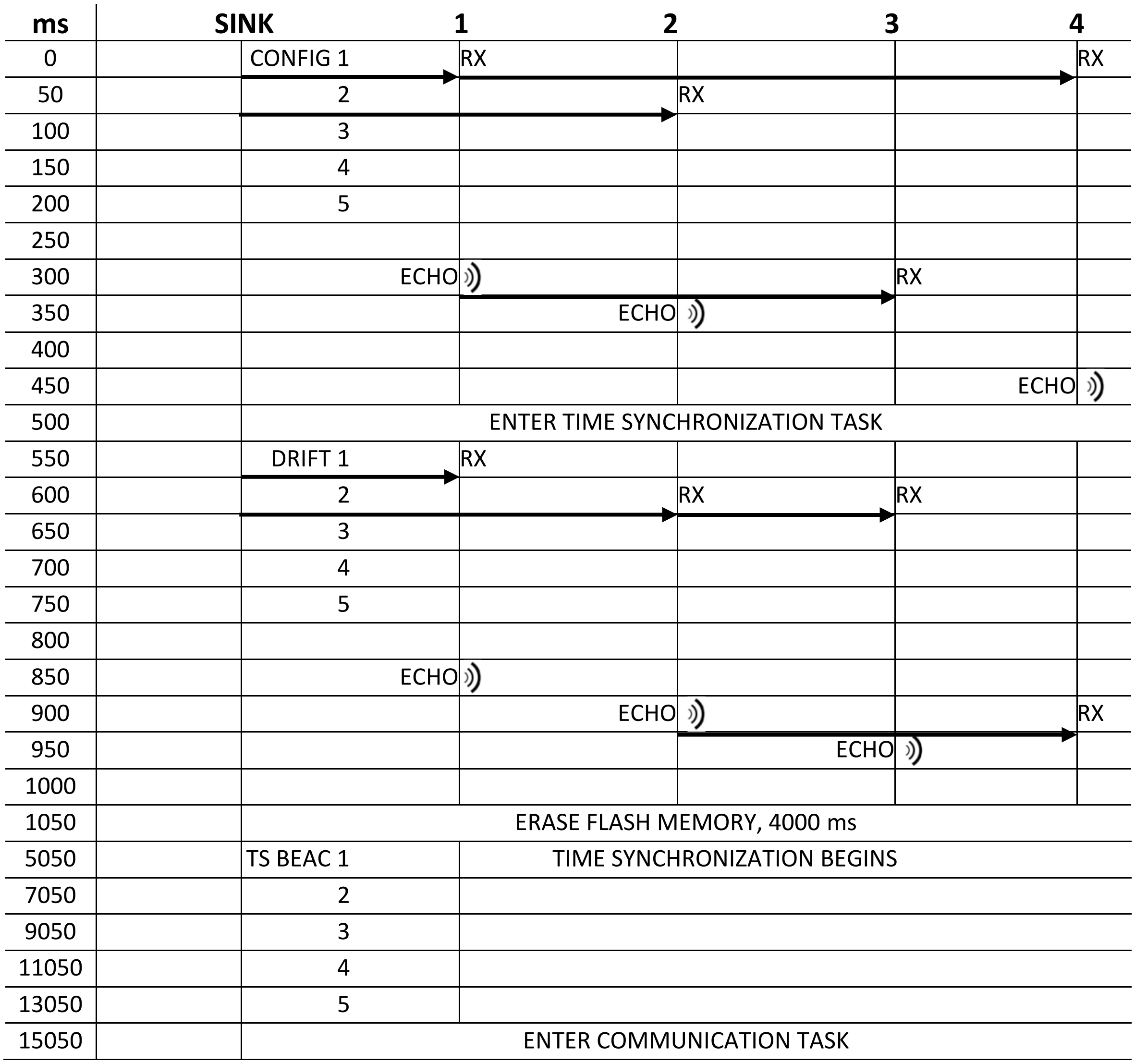
The end user defines some of the network parameters via a Matlab program which then transfers them to the sink node through universal asynchronous receiver transmitter (UART). The initial configuration packet holds information of the total number of nodes in the network, the number of packets to be broadcasted and the transmission interval, radio channel, and transmission power to be used. The configuration packet also contains the sink ID and a sequential number. The sink node broadcasts the configuration packets to the entire network and it is broadcasted five times in intervals of 50 ms to increase the probability of successful reception.

Table 5 illustrates the network configuration procedure. Nodes 1 and 4 receive the first configuration packet, node 2 receives the second and node 3 does not receive a configuration packet from the sink. At the reception of a configuration packet, the nodes set their own configuration parameters and calculate a backoff time before echoing the packet. Depending on the positions of the nodes, the echoing procedure increases the probability that every node will finally receive the configuration parameters. To ensure that every node echoes the configuration packet at a designated time slot, the backoff time is calculated from the sequence number of the packet and the nodes own ID. If a node receives the configuration packet from someone other than the sink and so avoiding collisions the echoing procedure is not performed.

After network configuration the nodes enter the time synchronization task. At the same time the configuration task is deleted so that resources of the MCU are not allocated by the ended task. Before network synchronization, information regarding the TS procedure is broadcasted to the nodes in the same manner as network configuration packets were transmitted. The time synchronization notification broadcasted by the sink, contains the total length of the TS procedure and the transmission interval of the TS beacons. Table 5, illustrates the TS notification from 500 to 1000 ms, after which the external flash memory is erased.

The TS procedure begins after the nodes have erased their flash memory and it is performed as described in section 3.2.4. The transmission interval parameter is copied in to the TACCR1 register of the MCU, to set the desired interrupt frequency. Thanks to the TS, the interrupts generated by all the nodes are synchronous and every time an interrupt is generated the node switches the state of the toggled pin. The resulting square wave represents the “heart beat” of the application. After the TS procedure is over, the application enters the intrusion detection task. During the task is running, the application layer monitors the

Table 5: Configuration and time synchronization of a network consisting of four nodes and a sink node. The configuration task is performed in the first 500 ms, which is followed by a time synchronization task. Time synchronization parameters are passed throughout the network from 500 to 1000 ms, after which flash memory is erased and the time synchronization is performed.



ms		SINK	1	2	3	4
0		CONFIG 1	RX			RX
50		2		RX		
100		3				
150		4				
200		5				
250						
300		ECHO			RX	
350			ECHO			
400						
450					ECHO	
500		ENTER TIME SYNCHRONIZATION TASK				
550		DRIFT 1	RX			
600		2		RX	RX	
650		3				
700		4				
750		5				
800						
850		ECHO				
900			ECHO			RX
950				ECHO		
1000						
1050		ERASE FLASH MEMORY, 4000 ms				
5050		TS BEAC 1	TIME SYNCHRONIZATION BEGINS			
7050		2				
9050		3				
11050		4				
13050		5				
15050		ENTER COMMUNICATION TASK				

"heart beat" and calls a transmission or reception function at each "beat". The time slots reserved for transmission and reception are determined by the unique ID's of the nodes, so that each node in the network has one transmission slot per cycle, and for the rest of the slots the node is in reception mode. The time slot for transmission is allocated for the node when the slot of the TDMA cycle matches the ID of the node.

Figure 14 illustrates the transmission and reception slots of two nodes in a network consisting of four nodes and a sink node. The first transmission is made by node ID 1. Meanwhile,

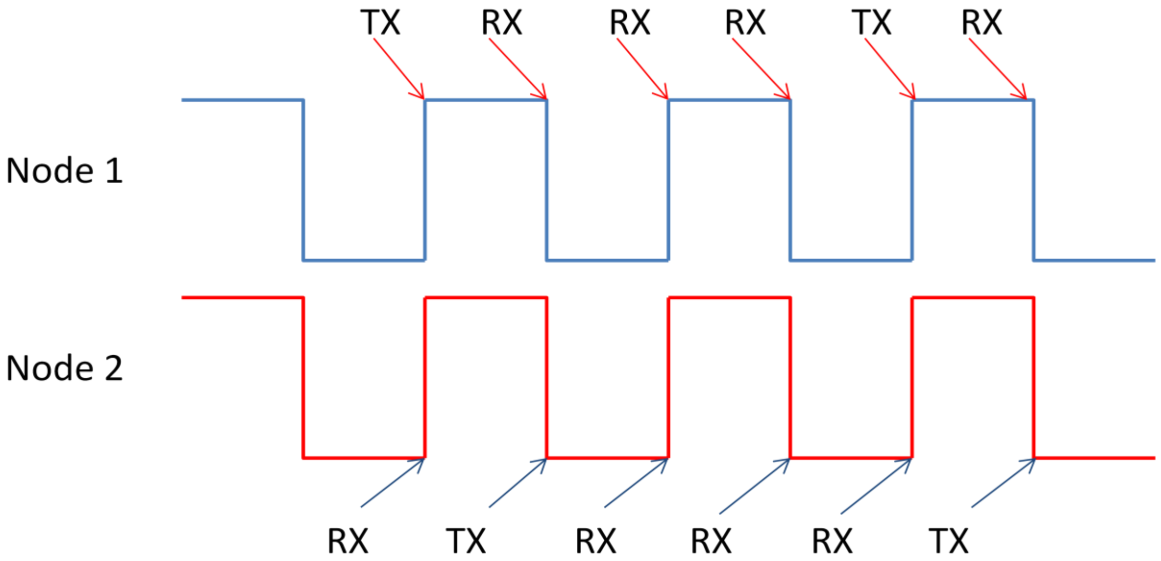


Figure 14: Square wave of nodes 1 and 2 in a network of 4 nodes. The reception and transmission slots are described using RX and TX in the corresponding order.

the other nodes are waiting for incoming packets from the transmitting node. After transmission, the node disables its radio to conserve energy. When the other nodes receive the packet, they disable their radio and compute the algorithm for intrusion detection. At the beginning of the 2nd TDMA slot, node ID 2 realizes that the slot is reserved for its transmission. The node enables its radio and broadcasts the packet. The broadcast of node 2 is followed by the broadcasts of nodes 3 and 4, after which the cycle ends and the procedure starts from node ID 1 again. A single node in the network functions autonomously communication wise, and as a result the network tolerates nodes failure and missed packets.

4.2 Evaluation of RSSI to detect movement

As stated in the previous section the nodes communicate in a TDMA fashion, where one node at a time broadcasts a packet while rests of the nodes listen for this broadcast. Each node includes its ID and the sequence number to the transmitted packet. The nodes are able to estimate the RSSI value of the received packet as described in section 3.1.2.1. In the first phase of the implementation, the nodes save all RSSI measurements, ID of the transmitter and sequence number of the packet to the sensor networking platforms external flash memory for offline analysis. In the next sections, the capability of the proposed system for detecting movements is analyzed.

4.2.1 Detecting movement between nodes

The first test is conducted using six nodes located on a line with intervals of 2 meters between every node pair. The transmission interval is set to 16 ms and a total of 1000 packets are broadcasted by every node. To reduce reflections from the floor, the nodes are elevated from the ground floor to a height of 1.1 meters using wooden podiums. The first measurements are conducted in a network where no movement is present in order to find the reference values for the links RSSI signal, while the second set of measurements are collected when a person is moving between nodes 1 and 2. Figure 15 illustrates the described testbed of six nodes and the trajectory of the moving person.

The upper image of Figure 16 shows the reference values of the RSSI when no movement is present. It can be observed that the RSSI measurements decrease as a function of distance as described in section 3.4.2. The RSSI measurements are steady with slight variation; $\sigma^2 <$ 1.25 dBm for each link. To study how a moving person effects the RSSI, the test is conducted again, with a person moving between nodes 1 and 2 as shown in Figure 15. During the test, the LoS of link 1-2 is crossed three times. The lower plot of Figure 16 reveals three instances where magnitude of the RSSI decreases remarkably. In addition, the links sense the LoS crossings simultaneously with this setup. The other links are consistent with the results shown in Figure 16, but for clarity the measurements of links 1-3, 1-4 and 1-5 are not shown.

The radio signals can be assumed to be the result of multiple multipath components. Radio signals coming from close-by nodes consist of few multipath components, being the power present in each component large. On the contrary, a radio signal received from a node located further away is a sum of numerous multipath components, being the power held by each component weak. Because of this, close by links reveal a much more evident drop in the received signal strength and the variance of the RSSI is large just before and after the drop.

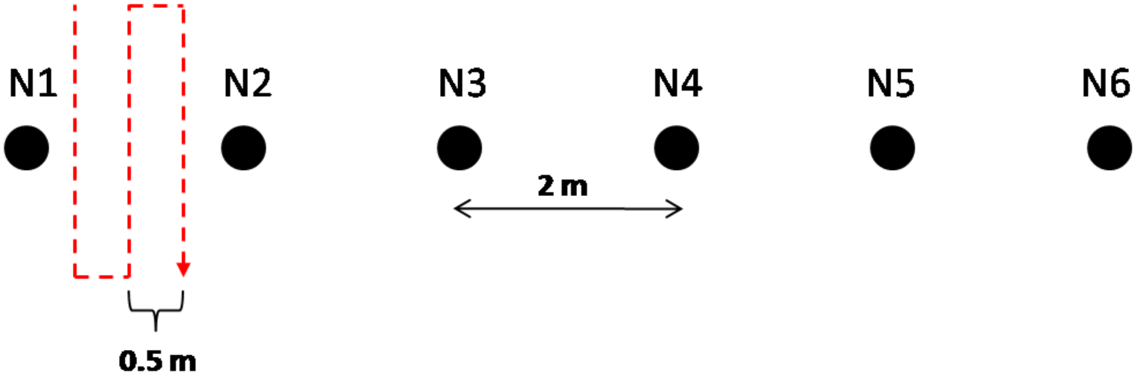


Figure 15: Placement of the 6 nodes and the path of the test person.

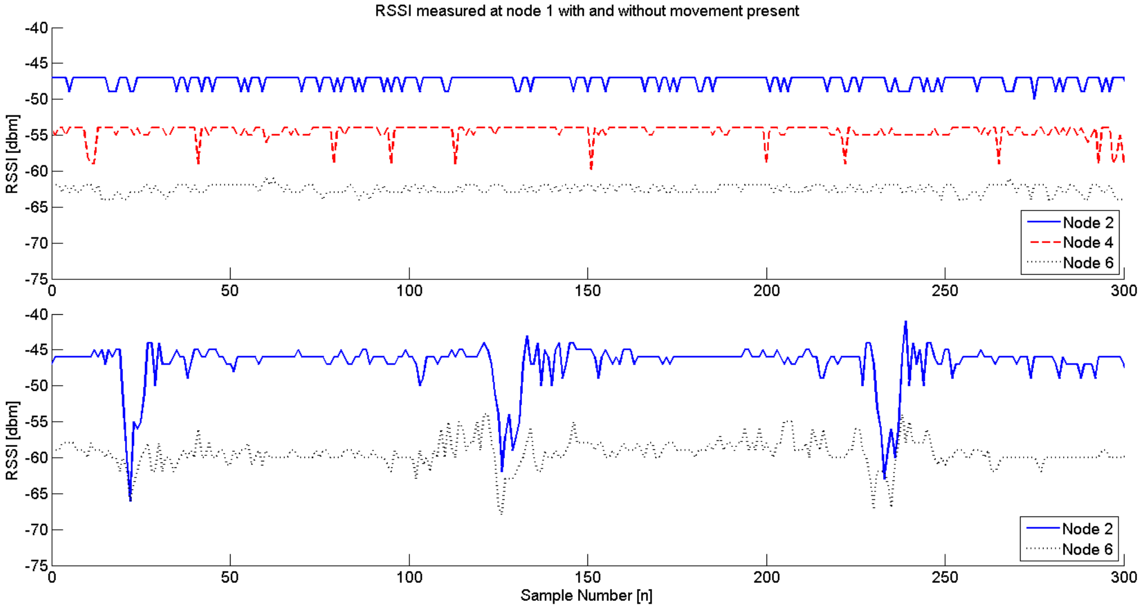


Figure 16: Measured RSSI values at node 1 with and without movement present in the close proximity of the network. The image above depicts to a situation where no movement is present where as the image below shows the affect of a person moving between the nodes. An obvious decrease in the RSSI magnitude can be perceived simultaneously from both nodes locating 2 and 10 meters away from the receiver.

Links further away show an increase in the variance of the RSSI lasting longer than in the close by links, but the LoS crossings do not cause such a significant decrease in the RSSI. From now on the area between the nodes where an intruder's body interferes with the radio signal causing a significant decrease in the received signal strength (shadowing) is denoted as sensitivity area of the link. Just before an intruder enters the sensitivity area and right after the sensitivity area is exited the RSSI measurements fluctuate (multipath fading) more than compared to static conditions (i.e. no movement in the close proximity of the nodes). This area is referred as the gray region of the sensitivity area. In this area the RSSI varies more than in static conditions, but the intruder's influence to the radio signal is not so evident.

In the test above, it was studied can movement be sensed between a node pair, and it was proven that in an open space the LoS crossings can be detected for at least distances up to 10 meters. In addition, increased variation in the RSSI measurements revealed movement in the close proximity of the links LoS. The test is conducted again, when a person moves in between and around the nodes in order to study the effect of movement to the RSSI when a person moves in the close proximity of the LoS. The trajectory of the test person is illustrated in Figure 17.

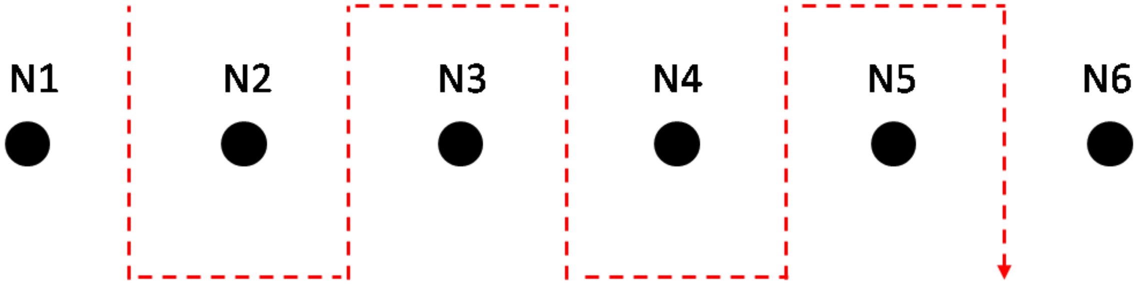


Figure 17: Placement of the nodes and the slalom trajectory. The first LoS crossing occurs between nodes 1 and 2. In total, LoS of link 1-6 is crossed five times.

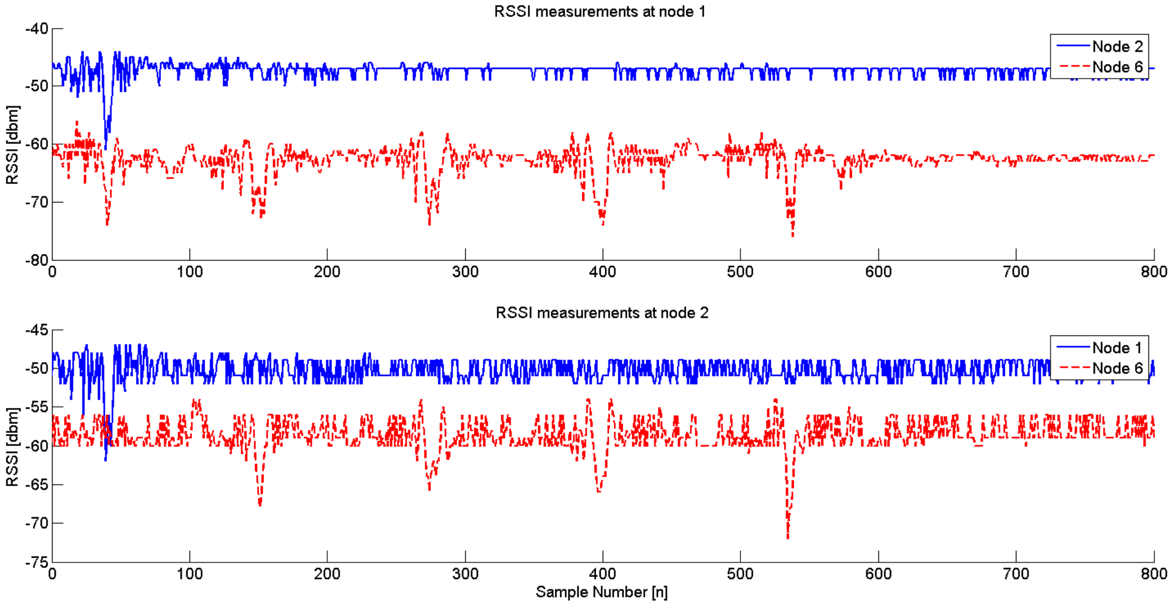


Figure 18 RSSI measurements of nodes 1 and 2. LoS crossings can be detected as decreases in the RSSI.

Measurements of links 1-2 and 1-6 are shown in the upper image of Figure 18 and measurements of links 2-1 and 2-6 are illustrated below. The LoS crossings of the “slalom” trajectory can be tracked throughout the measurements. Measurements of node 1 reveal the first LoS crossing between every link, but for example the measurements of link 2-6 do not reveal this. The second LoS crossing occurs approximately at sample 150, and both links (i.e. 1-6 and 2-6) can sense the intrusion. However, the link between nodes 1 and 2 does not show any decrease of the RSSI or increase in the measured variation. The three remaining LoS crossings can be seen from the measurements of links 1-6 and 2-6 approximately at samples 270, 400, and 540.

After sample 650 the test person exits the area, and by comparing the measurements after the person has departed the area to those that are taken between the LoS crossings, it can be seen that for most links the measurements correspond to each other. However, RSSI measurements of link 1-6 show abnormal behavior also in between the LoS crossings. The RSSI is steady after the intruder has left the area and by comparing this behavior to the RSSI measurements between the five obvious LoS crossings, it is evident that the radio signal is effected by movement also outside the sensitivity area. Anyhow, the reference behavior of the RSSI signal cannot be known beforehand and it is very sensitive to spatial position and orientation of the nodes. Due to these reasons, the LoS crossings are the only type of intrusions that will be considered from now on.

4.2.2 The effect of the surrounding environment to intrusion detection

So far the tests have been conducted in an open indoor environment in which walls and other obstacles were as far away as possible. The next test corresponds to the slalom trajectory described and illustrated in Figure 17 apart from a reception desk located parallel to the line on which the nodes are placed. The reception desk acts as a plausible reflection surface for the radio signals and lies 2.5 meters away from the nodes. The reception desk is made of granite and the dimensions of the reception desk are: 5.3·0.9·1.2 m (*l*·*w*·*h*).

The LoS crossings, illustrated in Figure 19 as circles, are derived by observing the node pair closest to the crossing point. For example the first LoS crossing is traced by examining

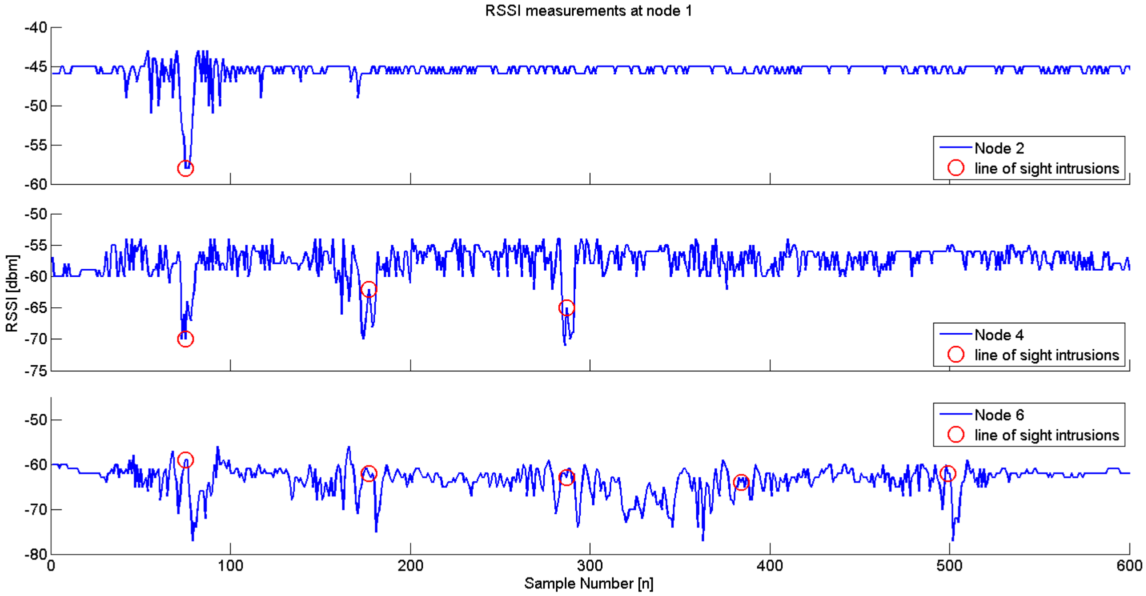


Figure 19 RSSI measurements of node 1. Results differ from those conducted in an area where no obstacles were present. Reflecting components are most evidently seen from the measurements between node 1 and 6.

the measurements of link 1-2. The moment of the second crossing can be captured by observing link 2-3 and so on. Links 1-2 and 1-4 behave as in the previous test, as can be seen from Figure 19, but the LoS crossings of link 1-6 are ambiguous since the variance of the measurements remains high also in between the 1st and 2nd LoS crossings, but also between the 3rd and 4th. It turns out that between these instances the intruder was moving in between the nodes and the reception desk. The intruder causes attenuation in the radio signals reflected from the reception desk and this is most evident between the 3rd and 4th LoS crossing. During this period the measurements fluctuate increasingly making the estimation of the LoS crossing impossible. Since the strongest decrease in the RSSI magnitude does not occur during the 3rd and 4th crossing but somewhere in between these instances, it can be derived that the strongest received components of link 1-6 are those reflected from the reception desk. The dominant components of links 1-2 and 1-4 are those that propagate along the line on which the nodes are placed. Otherwise also these links would reveal movement when the intruder is in between the nodes and the reception desk.

4.2.3 Estimating the sensitivity area of a link

In the previous sections it was shown that when a person is located in between a node pair or in an area where reflected components of the signal propagate, then the intruder can be detected utilizing the RSSI. In section 4.2.1 a term was introduced: sensitivity area of a link. In the following, an attempt is made to approximate the size of the sensitivity area, i.e. the perpendicular distance measured from the links LoS to the point in which the RSSI starts to react to the person moving closer to the nodes.

The tests are conducted using two nodes, at distances of 2, 3, and 4 meters. In the tests, the person always crosses the LoS a meter away from node 1. In the first run the path is directly in the middle, in the second the trajectory is a meter away from node 1 and 2 meters away from node 2, and for the last test the distances are 1 and 3 meters. The path followed by the person is controlled using markings on the floor which start at a distance of 3 meters away from the LoS and continue 3 meters away to the other side of the LoS. The person moves half a meter closer to the LoS every 5 seconds and when the person is a meter away from the LoS the step size is reduced to 0.25 m. After each transition the person is staying as still as possible in order to minimize the variance in the measurements.

The results of the tests can be seen in Figure 20. From the measurements it is not possible to state the exact size of the sensitivity area. However, an insight on the size of the area can be obtained. The largest decrease in the RSSI occurs in all measurements, when the person moves from the 0.25 m mark to the LoS. When the person moves from the LoS to the -0.25 m mark, the signal level increases but does not get back to the initial value. At the next 0.25

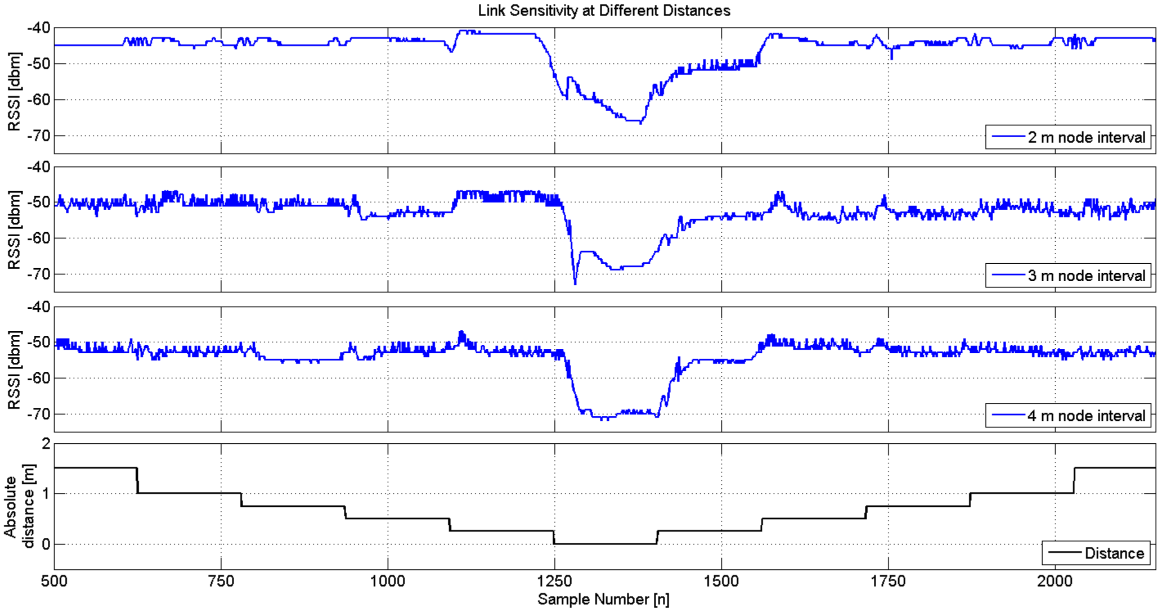


Figure 20 Sensitivity of the RSSI when an intruder is moving toward and away from the LoS. Measurements at node distances of 2, 3, and 4 meters are captured in corresponding order from top to bottom.

m step, the signal reaches the initial level. Even though the measurements of only node 1 are presented in Figure 20, the trends at both ends of the link are equivalent.

The silhouette of a human body is not homogenous, and in the tests, even though the feet were always on the floor markings the upper torso of the person could have fallen behind the marking. For example when the feet were placed on the 0.25 m marking, the upper body might actually have been 0.30 m away from the LoS. Similarly on the other side of the LoS, the distances would have been -0.25 m and -0.20 m. This fact would explain why the RSSI levels were not corresponding on the two sides of the LoS. Despite this, it can be clearly stated that the size of the sensitivity area is less than half meter away from the LoS. In the later sections an estimate of 0.25 m is used for the size of the sensitivity area, but in the future, additional tests should be conducted.

Before entering the sensitivity area described above, the measurements show increasing variation whenever a transition is made close by the nodes. At distance of 2 meters, a noticeable shift occurs when a step is made from 0.50 to 0.25 m. At distance of 3 meters, detectable changes in the signal occur at steps from 0.75 to 0.50 m and from 0.50 to 0.25 m. At the largest node distance, variation is already detectable in the transition from 1.0 to 0.75 m. The results imply that the gray region of the sensitivity area exists and is larger for nodes located further away from each other.

4.2.4 Approximating the velocity of an intruder

So far the only interest has been in detecting if an intruder can be detected inside the monitored area, but no attention has been paid to trying to localize the intruder or in estimating its velocity. After having defined the properties of the sensitivity area, an attempt to estimate velocity can be made. In the following, two different approaches to estimate the velocity are proposed. In the first, the knowledge of the sensitivity area is exploited to estimate velocity locally in the nodes. The other approach exploits information on the position of the nodes and measurements from all the nodes. The latter requires centralized processing but can be also executed in real-time.

4.2.4.1 Local estimation of velocity

From the time duration of an intrusion it is possible to estimate the speed component hat is perpendicular to the line connecting the nodes. The shorter the drop in the RSSI measures magnitude is, the faster the sensitivity area is passed through. By knowing the number of nodes in the network, the transmission interval, and the size of the sensitivity area (approximately 0.25 m) in both directions from the LoS, the velocity can be estimated as follows:

$$v_{\perp} = \frac{s}{\Delta n \cdot m \cdot \Delta t} \tag{12}$$

where s is the size of the sensitivity area, Δn *is* the intrusion length in samples, m is the number of nodes in the network, and Δt is the transmission interval. An experiment was made by using two nodes located two meters apart.

In the experiments the LoS was crossed with three different velocities and every velocity was measured three times. Figure 21 illustrates one LoS crossing with every velocity and the results are shown in Table 6. Duration t_{approx} is estimated from a video by extracting the time it takes to travel 4 meters. The test setup is not ideal but the results imply that the velocity estimates obtained with (12) are in the same range as the velocities estimated from the video recording. It is clear that with embedded processing it is plausible to state if the intruder is walking, jogging, or running.

There exists a drawback on estimating the velocity locally in the nodes, i.e. the transmission interval. The transmission interval sets the rate on how many measurements the nodes receive from a specific node in a certain time period. Decreasing the interval increases the number of packets the node receives while the intruder is in the sensitivity area, therefore making the estimate more accurate and vice versa when the transmission interval is increased. Not only the increase in the transmission interval but also the increase in the node number decreases the frequency at which the nodes receive packets from a certain node. In

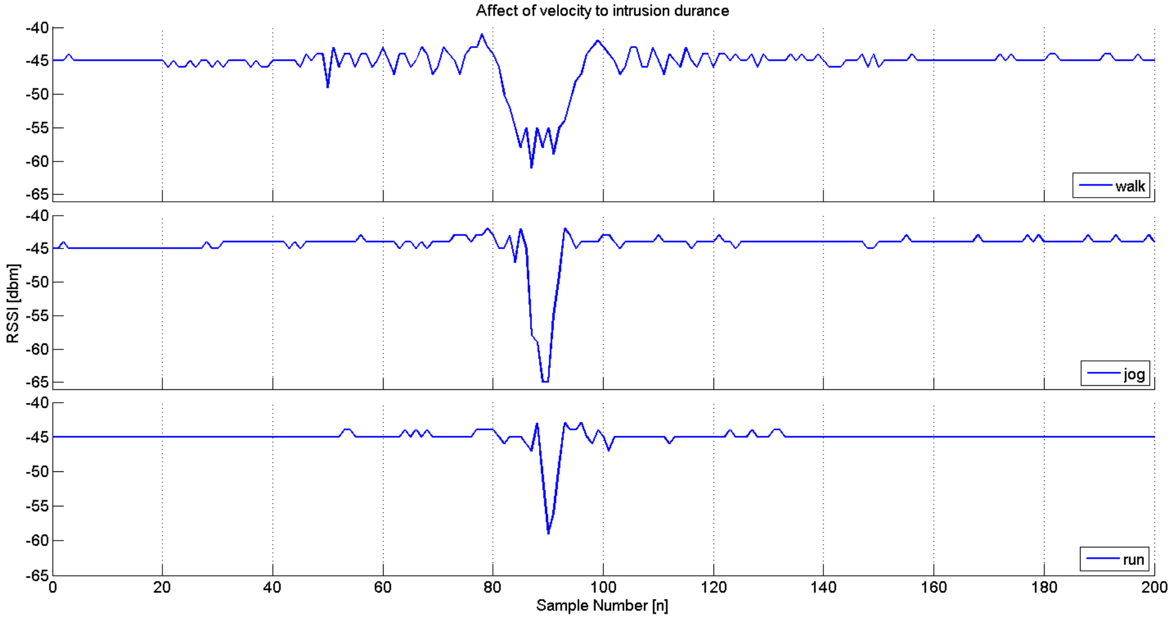


Figure 21 Duration of the intrusion at three different velocities. The faster the intruder advances, the less time the sensitivity area is occupied. An approximate value of the speed can be estimated from the duration of the intrusion.

Table 6 Speed estimates of the three different velocities. Speed is approximated both from video and by the node.

distance traveled = 4 m	**Measurement 1**	**Measurement 2**	**Measurement 3**
WALK			
duration t_{approx} (s)	6.28	5.75	5.16
speed in v_{approx} (km/h)	2.29	2.51	2.79
duration in samples (n)	21	21	19
speed in $v_{\perp}$ (km/h)	2.67	2.67	2.96
JOG			
duration t_{approx} (s)	2.40	2.11	2.20
speed in v_{approx} (km/h)	6.00	6.83	6.54
duration in samples (n)	8	8	9
speed in $v_{\perp}$ (km/h)	7.03	7.03	6.25
RUN SLOWLY			
duration t_{approx} (s)	1.56	1.52	1.51
speed in v_{approx} (km/h)	9.23	9.47	9.54
duration in samples (n)	5	5	6
speed in $v_{\perp}$ (km/h)	11.25	11.25	9.38

the tests above there was only 2 nodes in the network, and a packet was received every 32 ms. Having 12 nodes in the network and a measurement from a specific node would be received only every 192 ms, which would make accurate estimation already very challenging.

4.2.4.2 Offline velocity estimation

By knowing the positions of the nodes, it is possible to estimate the velocity from the duration of the interval it takes for the intruder to move from the sensitivity area of one link to the sensitivity area of another link. The velocity can be approximated as in 12, but this time the intrusion length Δn is extracted from multiple nodes. Figure 22 depicts the twelve nodes corridor testbed used in the test. As in the previous section, the measurements were made with three different velocities. The time length of the intrusions is derived from the RSSI measurements of nodes opposite to each other since their change in the RSSI is the largest. The lowest RSSI value is assumed to correspond to the LoS crossing of the link.

The measurements of three velocities are shown in Figure 23 below. The RSSI measurements show that the movement of the intruder can be tracked precisely. However, when the intruder was running (bottom figure), some links were not capable of detecting the LoS crossing. For instance, node 1 of link 1-7 missed the LoS crossing, but the reverse link 7-1 captured the crossing. Node 1 missed the LoS crossing due to the relatively high cycle duration.

In Table 7 t_{approx} is estimated from a video recording. From the results it can be stated that the speed estimates are in the same magnitude as the results obtained from the video. Table 7 includes also the speed estimates calculated locally by the nodes of links 1-7, 3-9, and 6-12. The results are not even near the approximated velocities and this is due to the large cycle time (192 ms). The nodes do not collect enough measurements while the person is passing the sensitivity area, and this fact leads to a low accuracy.

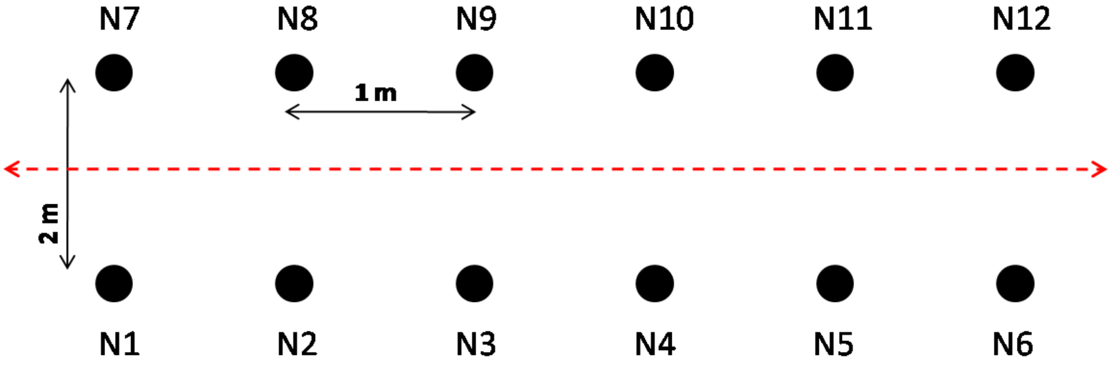


Figure 22 Testbed of 12 nodes and the described path illustrated with a red dashed line.

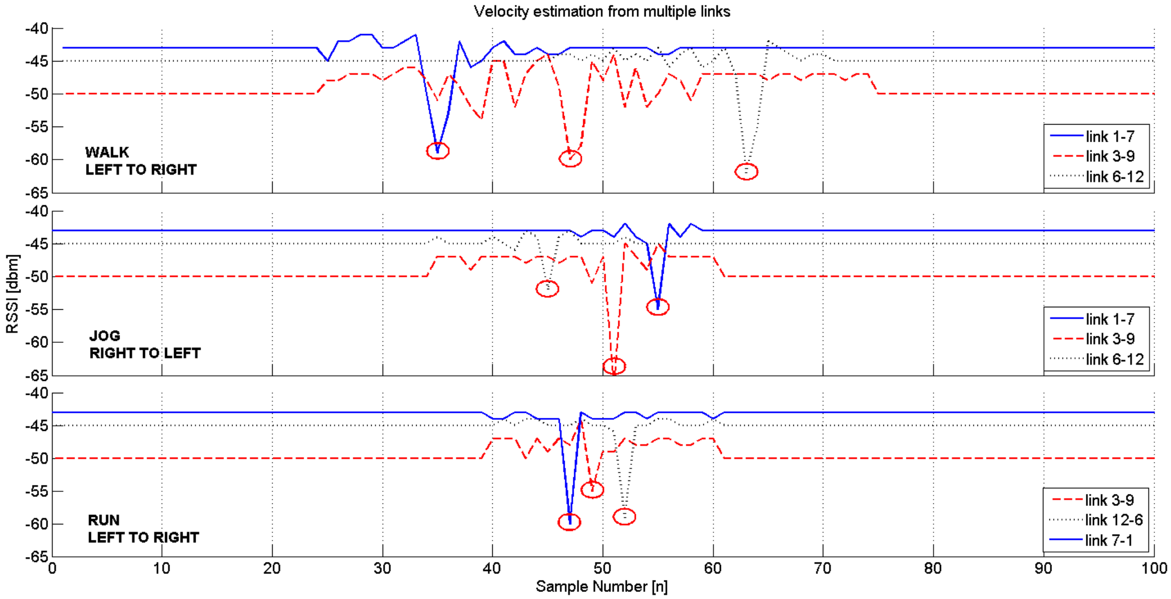


Figure 23 Estimating velocity using measurements from multiple links. Chosen links are opposite of one another and expose the LoS crossings most clearly. The running person is already moving so fast that link 1-7 doesn't record the LoS crossings, but the reverse link 7-1 can. Node 1 misses the LoS crossing due to the relatively slow cycle time (i.e. 12·16 ms = 192 ms).

Table 7 Speed estimates of the three different velocities. Speed is approximated both from video and from multiple links of the network.

distance traveled = 5 m	**WALK**	**JOG**	**RUN**
CAMERA ESTIMATE			
duration in t_{approx} (s) speed v_{approx} (km/h)	5.89 3.06	2.01 8.96	1.02 17.65
NETWORK ESTIMATE			
duration in samples (n) speed $v_{\perp}$ (km/h) Absolute error (km/h) Absolute relative error (%)	28 3.35 0.29 9.48	10 9.38 0.42 4.69	5 18.75 1.10 6.23
LOCAL ESTIMATE			
duration in samples (n) speed $v_{\perp}$ (km/h) Absolute error (km/h) Absolute relative error (%)	4 / 4 / 4 2.34 / 2.34 / 2.34 0.72 / 0.72 / 0.72 24 / 24 / 24	3 / 2 / 2 3.13 / 4.68 / 4.68 5.83 / 4.28 / 4.28 65 / 48 / 48	0 / 1 / 0 NaN / 9.38 / NaN NaN / 8.27 / NaN NaN / 47 / NaN

4.2.5 Exposing various movement types

In the tests described in sections 4.2.1 through 4.2.4, the nodes were elevated from the ground floor (1.1 m). The following test was conducted using the same setup of Figure 22 but this time having the nodes also on the floor. Three different types of movement were studied: bowing down (1), crawling on all fours (2), and by crawling on the ground (3). The influence on the RSSI can be observed in Figure 24.

When the nodes were elevated from the floor the passing of the intruder did not influence the RSSI. The elevated nodes were not able to detect any of the three movement types since the links sensitivity area was passed from underneath. However, when the nodes were placed on the floor, all three movement types were correctly detected. By crawling, the person influences the links RSSI measurements for the longest time period and it can be derived from the measurements that crawling was the slowest way to move. The fact that all movement types can be detected when the nodes are placed on the floor is beneficial, since in military scenarios the nodes will most probably be thrown on the floor.

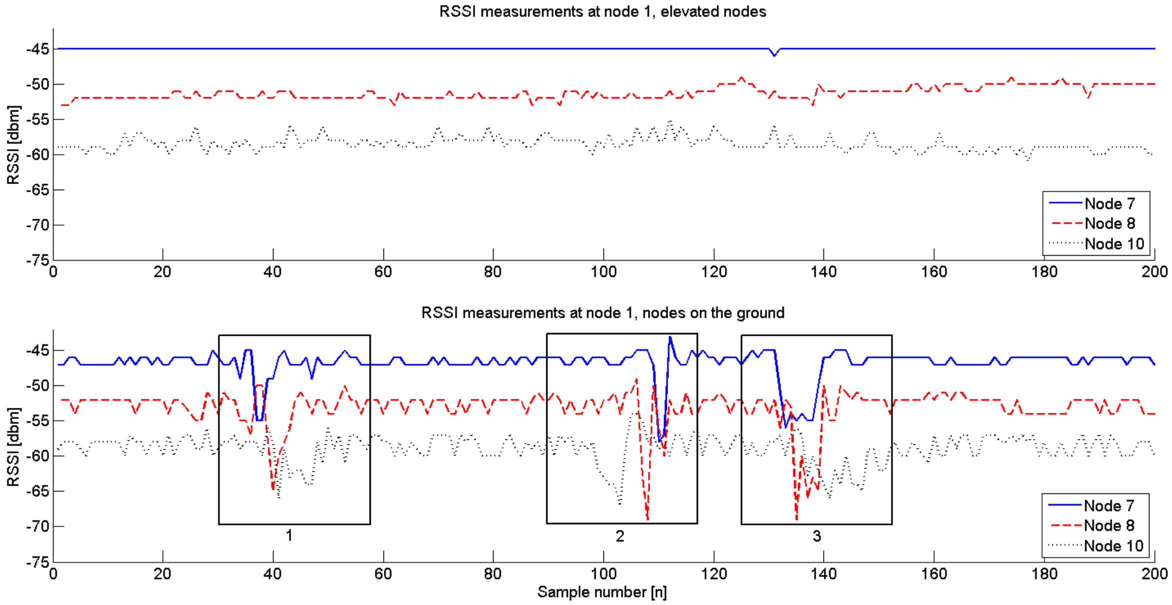


Figure 24 Detecting various movement types with elevated nodes and nodes on the floor. The first intrusion from the left is when the test person is squatting down (1), second in turn is being crouched down on ones knees (2) and the last intrusion is by crawling on the ground (3).

4.3 Intrusion detection using RSSI measurements

An explanation of the RSSI characteristics and how it behaves when a moving person was in the sensitivity area of the link was made in section 4.2. In this section an embedded algorithm executed locally in the nodes to detect intrusions is presented. Design features for the algorithm are listed below:

- Sensitivity to the decreases in RSSI magnitude when intrusions occur.
- Other fluctuation of the RSSI should be neglected.
- The surrounding environment shouldn't affect the reliability, and the algorithm should work in spite of the nodes being close by or far away from each other.
- Computation of the algorithm should consume as little time as possible.
- Allocation of the sensor networking platform's scarce resources should be avoided.

4.3.1 Embedded algorithm for intrusions detection

When there are no moving people in the monitored area, transmitting to the base station raw RSSI measurements would represent a considerable waste of power. Thus, detecting intrusions by locally processing the RSSI measurements in the nodes and then transmitting to the base station significant alerts, not only reduces the communication overhead, but also the need at the base station of processing measurements which do not hold interesting information.

The proposed embedded intrusion detection algorithm is based on the fact that when motion occurs nearby a wireless link, its multipath components are obstructed, and this inevitably introduces variance in the RSSI. Variance has been previously identified as a promising measure by Patwari and Wilson (2010) to detect movement in areas monitored by a WSN. Figure 25 presents the measurements of links 1-3 and 1-6 of the "slalom" test conducted in section 4.2.1, and the sliding variance of the RSSI measurements over a time window of 20 samples. The results imply that variance increases manifolds at intrusion instances and remains fairly low elsewhere. In the following a method to calculate sliding variance recursively is introduced, after which the logic to detect intrusions locally in the nodes is presented.

The change of the *n*-th RSSI measurement of link *i-j* is calculated as follows:

$$\Delta x_{i,j}[n] = x_{i,j}[n] - f_{i,j}[n-1] \qquad (13)$$

where $x_{i,j}[n]$ is the current raw RSSI measurement of link *i-j* (being nodes *i* and *j*) and $f_{i,j}[n-1]$ is the value of the previous filtered RSSI measurement. The filtered value of sample *n* is

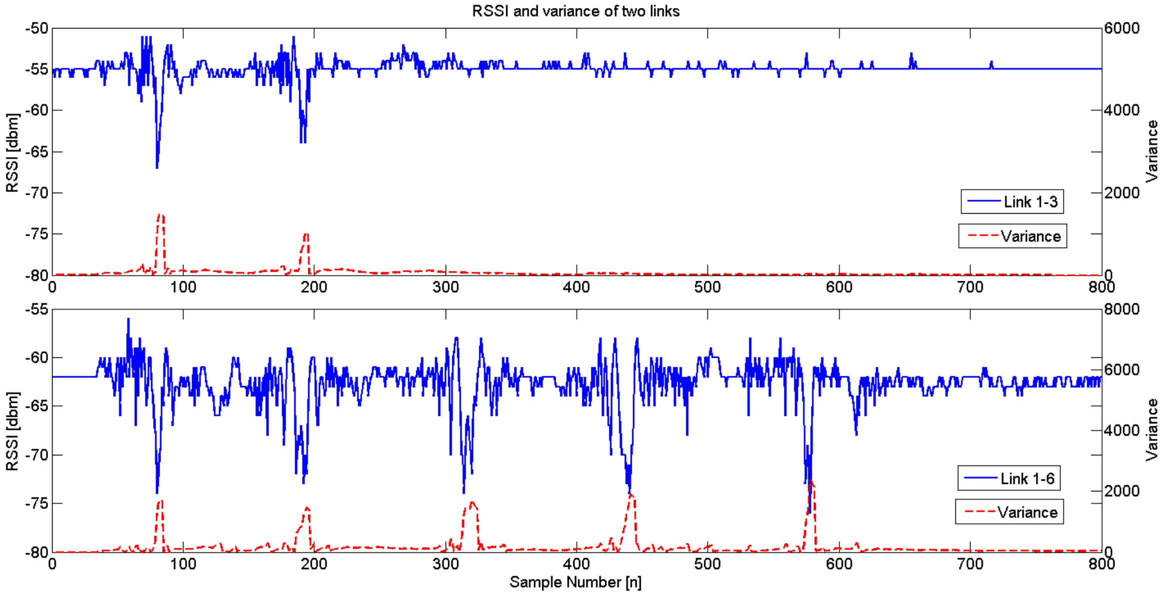


Figure 25 RSSI of links 1-3 and 1-6 and sliding variance of the measurements. Variance is calculated over a time window of 20 samples.

calculated with a first order low-pass filter:

$$f_{i,j}[n] = \alpha \cdot x_{i,j}[n] + (1-\alpha)\, f_{i,j}[n-1] \tag{14}$$

where $\alpha \in [0,1]$ is the smoothing factor and $f_{i,j}[0] = x_{i,j}[0]$. The sliding sum of the squares of the current and previous measurements is then calculated as follows:

$$\Sigma^2_{i,j}[n] = \Sigma^2_{i,j}[n-1]\left(1 - \frac{1}{n_{forget}}\right) + \Delta x_{i,j}[n]\left(x_{i,j}[n] - f_{i,j}[n]\right) \tag{15}$$

where the forgetting factor n_{forget} defines the size of the window over which the variance is calculated and $\Sigma^2_{i,j}[0] = 0$. In equation (15), the first term subtracts the average of the sum of squares over the sliding window when a new value is computed. However, to calculate the exact value for the sliding sum of squares would require saving entire RSSI measurements time-histories over the sliding window, leading to an excessive usage of the RAM memory of the MCU. The sliding variance of link *i-j* at sample *n* is:

$$\hat{\sigma}^2_{i,j}[n] = \Sigma^2_{i,j}[n] / \left(n_{forget} - 1\right) \tag{16}$$

In the intrusion detection algorithm a second variance, calculated over a shorter time window, is introduced to increase the reliability of the algorithm. The effect of a person moving in the close proximity of a link causes an increase in variance of the otherwise stable RSSI measurements. The short-term variance $\hat{\sigma}^2_{short}$ reacts more rapidly to these changes. An intrusion alert is raised when the short-term variance exceeds a pre-defined threshold (set to 5 in the experiments to avoid alerts caused by noisy RSSI measurements) and simultaneously doubles the long-term variance $\hat{\sigma}^2_{long}$. The algorithm considers the intrusion ended, and thus kills the alert, when a raw RSSI measurement returns above the filtered RSSI value stored at the beginning of the intrusion.

The flow of the embedded RSSI processing algorithm is presented in Figure 26 and the alerts raised by the algorithm are shown in Figure 27. The alerts are raised correctly by the nodes at time instances when LoS crossings occur. The flat line of the alert level indicates no alerts, and peaks of the alert line indicate intrusions in the sensitivity area of the link.

```
Compute short- and long-term variance;

If $Trigger_{i,j}$ is on:
    If $x_{i,j} > Trigger_{i,j}$:
        Old alert over, reset $Trigger_{i,j}$, $\Sigma^2_{short}$ and $\Sigma^2_{long}$ for link i-j;
    Else:
        Old alert still on, set $Alert_{i,j}$ on;
    EndIf
EndIf
If ($\hat{\sigma}^2_{short} > 2 \cdot \hat{\sigma}^2_{long}$ and $\hat{\sigma}^2_{short} > Threshold$):
    If $Trigger_{i,j}$ is off:
        New alert identified, set $Alert_{i,j}$ and $Trigger_{i,j}$;
    EndIf
ElseIf $Trigger_{i,j}$ is off:
        Set $Alert_{i,j}$ off;
EndIf
If $Alert_{i,j}$ on:
    $Alert_{i,j} = \left|\hat{\sigma}^2_{short} - \hat{\sigma}^2_{long}\right|$
EndIf
```

Figure 26 The flow of the embedded intrusion detection algorithm.

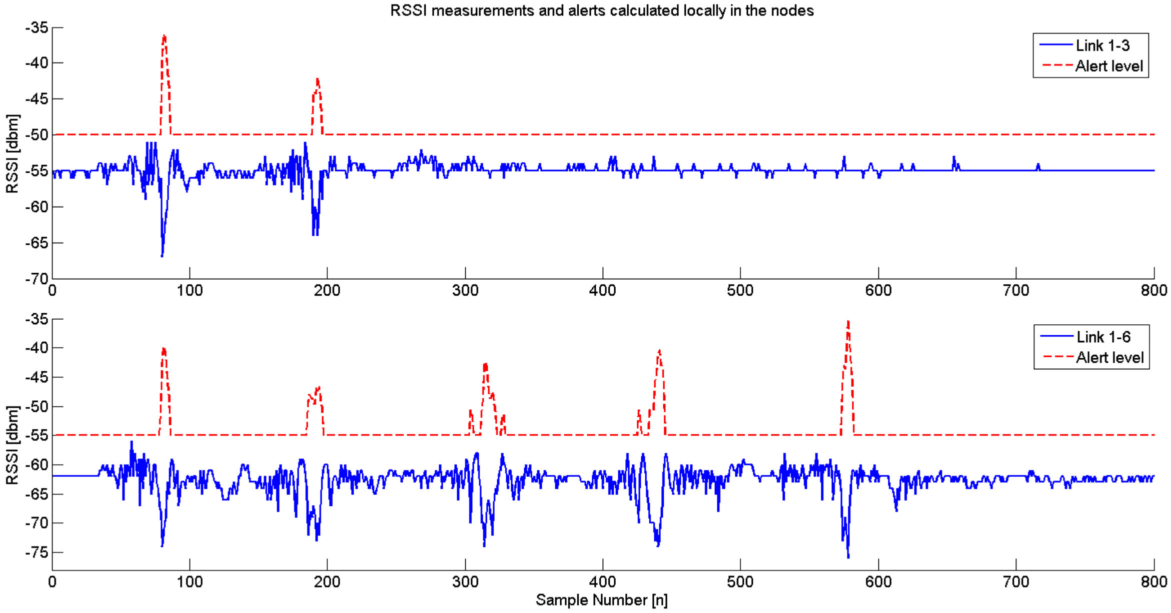
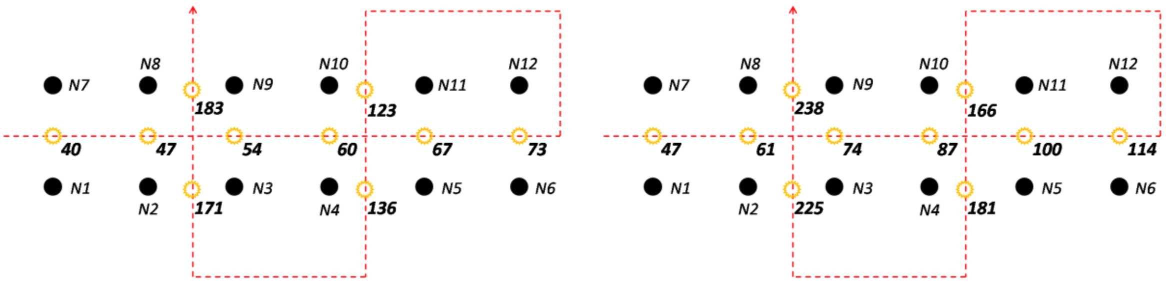


Figure 27 RSSI measurements of links 1-3 (above) and 1-6 (below) of the "slalom" trajectory test conducted in section 4.2.1. The locally calculated alerts are illustrated with the dashed red line.

4.3.2 Performance evaluation of the embedded intrusion detection algorithm

In the previous section the embedded algorithm run by the nodes to detect intrusions in real-time was introduced and evaluated through the "slalom" test. In the test, path of the intruder was fairly simple and the maximum nodes distance was rather small, only 5 meters. In the following, a more complex test is performed to further evaluate the performance of the algorithm.

In the tests, two corridor type testbeds were considered. The tests were conducted using two different nodes interval (i.e. 1 meter shown in Figure 28 (a) and 2 meters shown in Figure 28 (b)). The figures also represent the path followed by the intruder and the time instants corresponding to the LoS crossings. Figure 29 shows the RSSI measurements and alerts raised by links 6-7 and 6-10 in both testbeds. In the smaller corridor, node 6 triggered the alerts with nodes 7 and 10 at correct time instances. Also in the larger corridor all LoS crossings were detected, but link 6-7 also shows an additional decrease in the RSSI between sample 50 and 100. This additional peak is caused by the imperfect radiation pattern of the omnidirectional antenna illustrated in Figure 30. The radio signal propagation is stronger in particular directions from the antenna. During the tests the intruder walked through the "lobes" and caused two significant decreases in the radio signal strength even though the LoS was crossed only once. Nodes close by did not experience this phenomenon and therefore they gave a more precise estimate of the intruder's actual position. Since the embedded algorithm is more precise for links that are close to one another, alerts raised by close-by links should outweigh the alerts made by links with larger nodes interval.



(a) (b)

Figure 28 Two corridor testbeds. Size of corridor (a) is 2 x 5 meters and the horizontal nodes interval is 1 meter, whereas corridor (b) is 2 x 10 meters and the horizontal nodes interval is 2 meters. In the figures sample numbers are presented for a number of known locations and they are derived with the same method as in section 4.2.2. A reception desk locates 2.5 meters away from the line connecting nodes 1 through 6 and is parallel to the line.

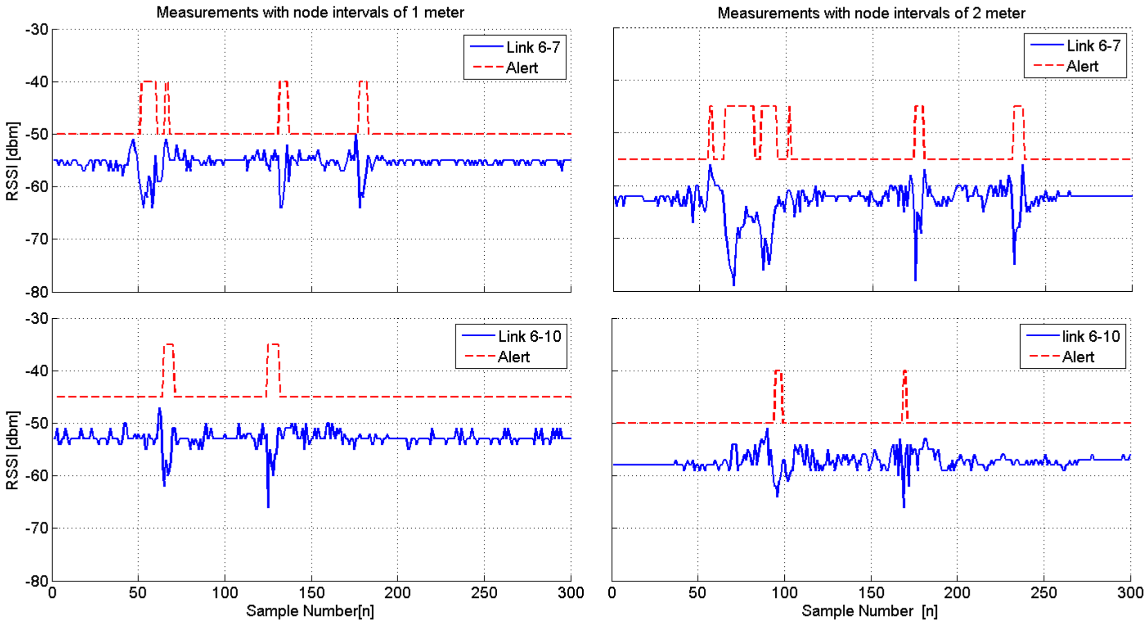


Figure 29 Measurements and alerts raised by the node for links 6-7 and 6-10 in the two comparable corridor testbeds. Alerts in corridor (a) are raised at correct time instances when the LoS crossings occur. With larger node distances the alerts are not raised with the same accuracy. Link 6-7 experiences two LoS crossings between samples from 50 to 100 even though the link is crossed just once.

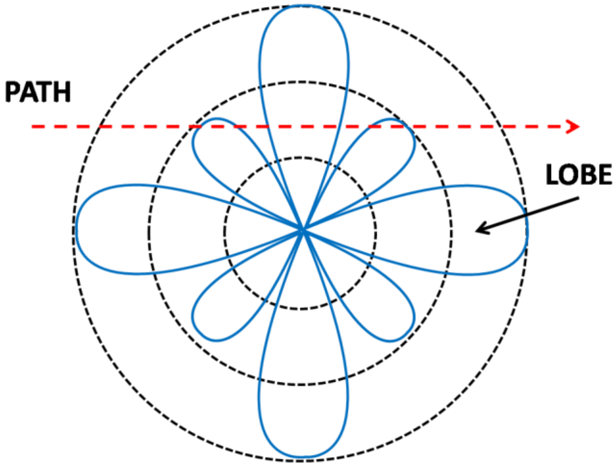


Figure 30 Radiation pattern of an imperfect omnidirectional antenna.

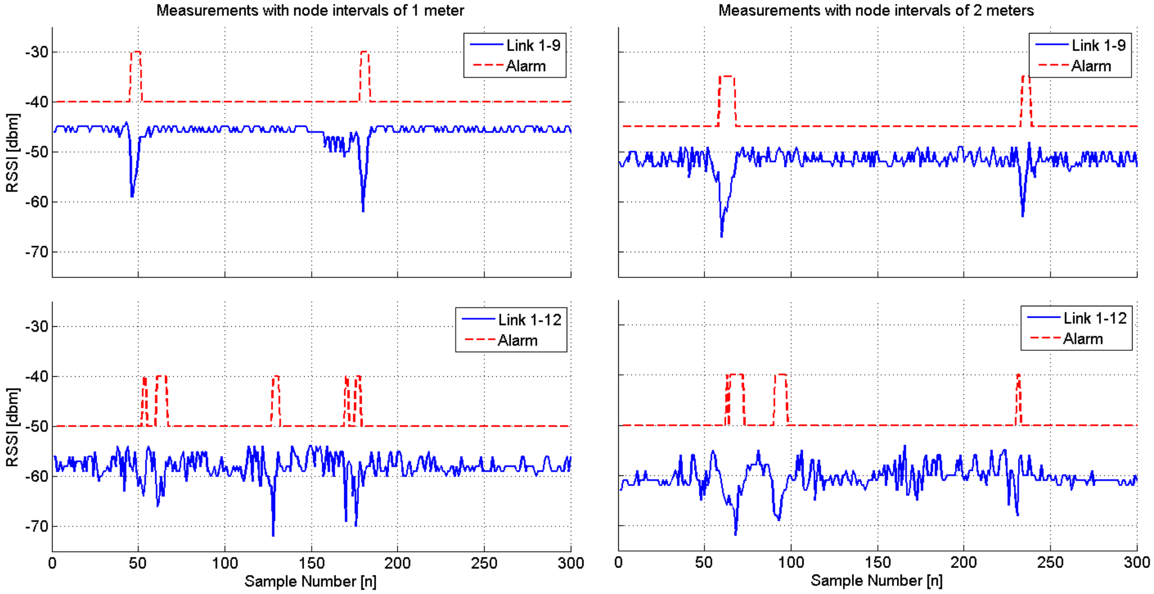


Figure 31 Measurements and alerts raised by node 1 for links 1-9 and 1-12 in the two comparable corridor setups. Alerts in the corridor (a) are raised at correct time instances when the LoS crossings occur. With greater node distances the alerts are not raised with same accuracy and link 1-12 also misses one LoS crossing at sample number 170. At this time the variance increases considerable but not enough to raise an alert. Also between cycle rounds 50 and 100, link 1-12 experiences the same phenomenon as link 6-7 in figure 21. The alert magnitudes are normalized to 10 to clarify the illustrations.

Measurements of Figure 31 support the previous results. The RSSI measurements collected by close-by links were less noisy. Link 1-12 (also links 12-1 and 7-6 even though they are not illustrated) also experienced the effect of the imperfect omnidirectional antenna. In addition, link 1-12 missed one LoS crossing at sample 170. However, the LoS crossing was detected by link 12-1. It is obvious that with a smaller nodes interval the alerts are raised more accurately and tracking the location of the intruder is more precise, but to cover the same area as with the larger nodes interval would require more nodes.

By using the described embedded algorithm, intrusion detection was accurate with nodes interval up to 5 meters. With greater distances some LoS crossings were missed but these situations were conflicting. For example link 1-12 missed a LoS crossing at sample 170, but the RSSI measurements show that the magnitude of the signal doesn't decrease significantly, only the variation of the RSSI signal increases. The embedded algorithm could be designed to be more sensitive, but this would also increase the number of false alerts.

In some of the measurements there were instances where alerts were raised even though a LoS crossing did not occur. These false alerts were possibly caused by reflections from the reception desk and from other obstacles surrounding the network. The algorithm responded to these fluctuations by raising the alert even when nobody was close-by the LoS. This issue is not related to the algorithm design, but rather a problem due to spatial positioning of the nodes and to the effect of indoor environment on radio signal propagation. Centralized processing of the aggregated alerts can cope with these false alerts, since more information is available and the wrong alerts can be filtered out.

4.4 Real-time intrusion detection in WSNs

In section 4.3 the real-time algorithm executed locally in the nodes to detect intrusions was derived. The alerts raised by the nodes have to be forwarded to the sink node in order to inform the end user of the intrusions. This section is structured as follows: after the application timeline is analyzed, the method to transmit alerts to the sink node is explained. From the aggregated data received at the sink, estimating the position and trajectory of the intruder becomes possible. Section 4.4.3 evaluates the performance of the DFL system using four different testbeds; 2 corridor type testbeds, already introduced in 4.3.2, and two square type testbeds where nodes are placed on the premises of a square. The sides of the area are equal of length and on each side the same amount of nodes are placed.

4.4.1 Application timeline analysis

In section 4.1, communication procedure of the application was explained on a general level, but the operations executed during transmissions and receptions were not exhibited. In the following a detailed analysis of the transmission and receptions slots is presented. The timeline of the application is analyzed by toggling the external pins of the Micro.2420 sensor networking platform. The measurements are conducted using an Agilent 16902A logic analysis system, equipped with a 16760A state and timing module capable of acquiring signals at rates up to 1.5 GHz. A total of eight channels are measured from two nodes simultaneously with a sampling rate of 400 MHz.

Figure 32 shows a single transmission slot and the corresponding reception slot. In the beginning of the transmission slot, the application layer pushes the data to be transmitted into a transmission buffer and just before the packet is broadcasted the node switches its radio on. The packet travels through the layers of the stack and it takes 3.872 ms in average to reach the MAC layer. From Table 8 it can be seen that the durations of different operations vary considerably; this fact is due to the interrupts generated by the multiple parallel tasks executed at different layers of the stack by the MCU. The packet is finally forwarded from the MAC layer to the physical layer, where the actual broadcast is made. Once the transmission has occurred the radio is turned off. The radio is on for 7.637 ms in average during the transmission slot (approximately 40 % of the slot length).

In the beginning of a reception slot the node turns on the radio and begins to wait for the expected packet. The packet is received at the MAC layer 6.247 ms in average after the beginning of the reception slot. The large difference between the minimum and maximum times to receive the packet is due to the length variations of the transmission procedure.

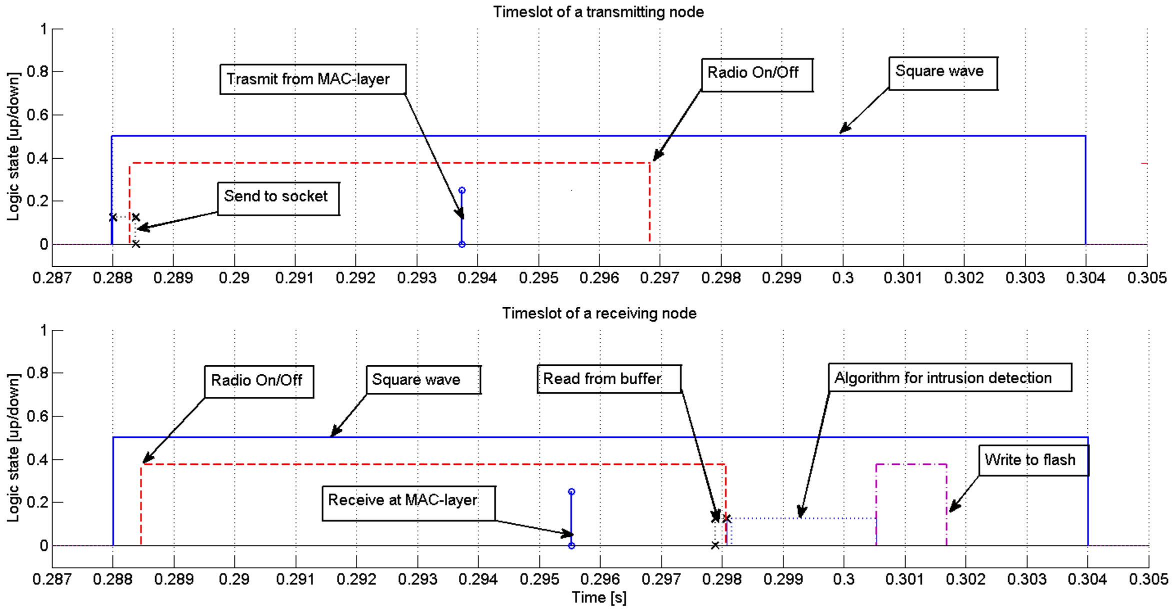


Figure 32 Transmission and reception slots of the application. The most time consuming procedure is for the packet to reach from the transmitter's application layer to the receiver's application layer, which takes 8.644 ms in average. In the worst case scenario, this procedure can take up to 10.595 ms, which is approximately 2/3 of the TDMA slot length.

Table 8 Average starting time of the operations in the transmission and reception slots shown in the 2nd column. If all columns are filled or average start time is empty then the minimum and maximum values refer to the duration of the operation. If duration slot is empty the values refer to the minimum and maximum from the beginning of the TDMA slot.

values in ms	**Start Average**	**Duration Average**	**Min**	**Max**
Transmission				
Push to buffer	0.017	0.4086	0.373	0.48
Radio ON	0.319	7.637	4.625	9.446
Packet to MAC	-	3.872	2.036	5.759
Packet at MAC	4.296	-	2.523	6.146
Reception				
Radio ON	0.833	8.010	6.426	10.311
Packet at MAC	6.247	-	4.548	8.097
Packet at APP	8.644	-	6.914	10.595
Pull from buffer	-	0.211	0.184	0.292
Algorithm	8.951	2.151	1.858	2.432
Flash write	11.121	-	9.073	13.206
Write to flash	-	-	1.155	1.256

The packet is then transported through the stack up to the application layer. The transfer from the MAC layer to the application layer takes approximately 2.4 ms and it is nearly constant, being 2.362 ms the fastest execution of the procedure and 2.492 ms the slowest. Once the packet is received at the application layer the radio is turned off. In average, during the reception slot the radio is enabled for 8.010 ms (approximately 50% of the reception slot length). After the radio is disabled the operations of the intrusion detection algorithm are executed in 2.151 ms in average. For debugging purposes, the RSSI measurements and the calculated alert magnitudes are saved in the external flash memory; this operation takes 1.208 ms in average to be executed. The writing isn't however performed every time a packet is received. The data are temporarily stored into an array and when all its 60 bytes are used the data are then written in a page of the flash memory at once. Thus in the tests, the flash operation is executed every 15th packet reception. The maximum time length of the interval from the beginning of the transmission procedure to the end of the intrusion detection algorithm and the saving of the data is 14.46 ms, which sets the limit for the transmission interval. The 16 ms transmission interval is chosen to assure that the receiving nodes are ready when a new TDMA slot begins.

4.4.2 Alert aggregation and processing for intrusion detection and tracking

The alerts are transmitted to the sink node together with the broadcasted packets used to detect intrusions. The first four bytes of the packets include the packet identifier, ID of the transmitting node and the packet sequence number, as explained in section 4.1. If a node has detected an intrusion in one or more links, then this information is included in the broadcasted packet by adding the ID(s) of the node(s) with whom the alert was (were) detected with and the alert(s) magnitude(s). These two fields are included in correspondence to every alert raised by the node.

The sink node is continuously listening to the same radio channel the other nodes are using for communication. The sink node interprets every received packet and if the length of the packet's payload exceeds four, then the sink node is aware that there is information concerning alerts in the packet. The payload of a packet including alerts is shown in the following structure:

Packet type:	*60*
TX node ID:	*1*
Seq. number:	*0 (8 MS bits) | 99 (8 LS bits) = 99*
Alert node ID:	*2*
Alert magnitude:	*87*

The transmitting node has ID 1, the packet sequence number is 99, and node 1 has detected an alert with node 2.

The sink node transfers the received information via UART to a Matlab application, where data are processed. The data are extracted from the received packet and reformed into a string to which a time stamp is added. The string is passed to a function which then calculates the position estimate from the aggregated alerts. The string extracted from the packet described above is:

ALERT: 60-1 2-87 at time: 13:48:25:821.

The alerts raised by the nodes are interpreted as follows to estimate the position of the intruder. Figure 33 (a) illustrates one node triggering an alert with three different nodes. Most likely, the intruder is located within the area that spans between the nodes. Alerts raised by multiple nodes within a short time window can be seen in Figure 33 (b). The most likely position of the intruder can be determined from the intersection points of the active alert links, as shown in Figure 33 (c). The intersection points are illustrated as circles and the position estimate (cross) is calculated with a weighted average from the intersection points. In the computation, a weighted average is used to emphasize links with greater alert magnitude.

When an intrusion occurs, the Matlab application is likely to receive multiple alerts from the sink node over a short time window. Since the alerts from multiple links give a more

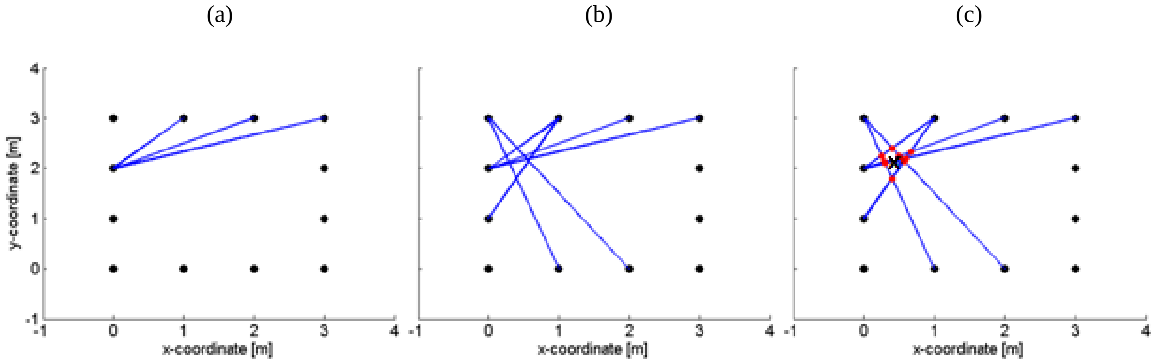


Figure 33 Formation of a position estimate. Alerts detected by a signal node presented in (a). Multiple alerts from three different nodes presented in (b). The intersection points of the alert links, shown in (c), confine the area where the intruder is located. Weighted average is used to emphasize links with greater alert magnitude.

precise picture of the monitored area, the alerts are not interpreted singularly one by one. Once an alert is received, the application waits for other alerts for 100 ms, which is approximately half of the TDMA cycle time. When the 100 ms time window expires the received alerts are aggregated and processed to estimate the position of the intruder. This is done by following four distinct rules:

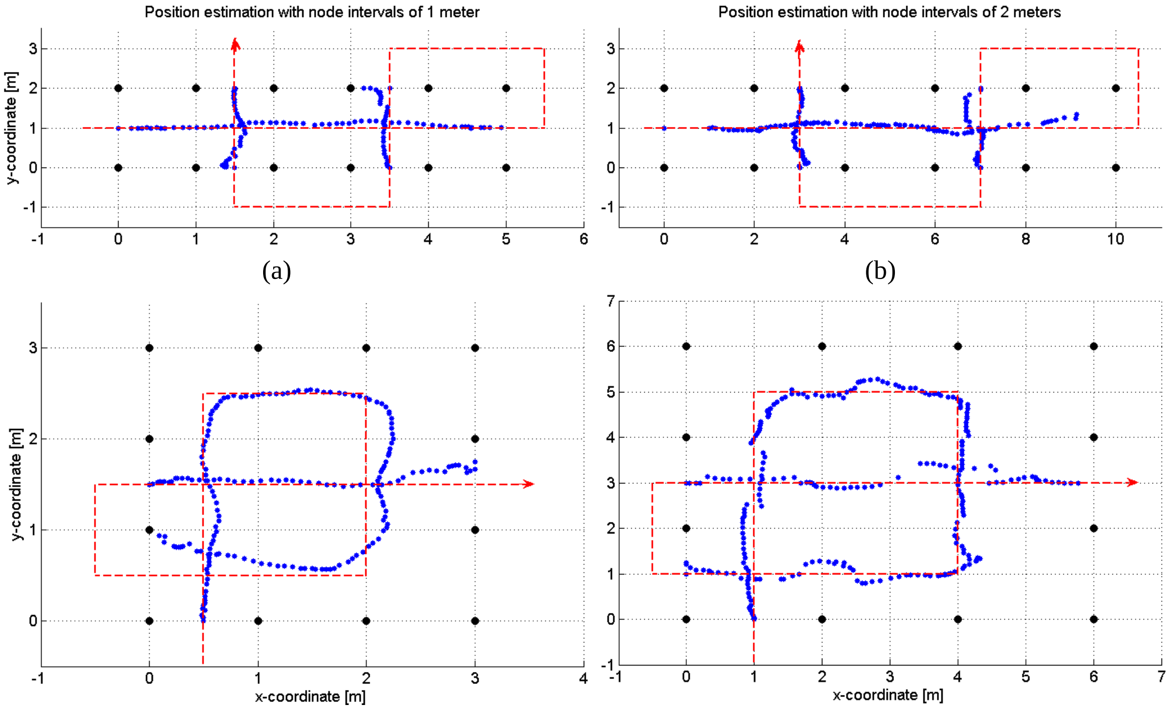
- A single alert within the 100 ms time window is considered as a false alert and it is neglected.
- Only the link with the shortest distance is considered if alert links are overlapping. Other alerts are neglected and their alert magnitudes are summed to the magnitude of the shortest alert link. The position estimate is set at halfway of the link.
- In the case in which alert links do not intersect, but the node records alerts in multiple links as in Figure 33 (a), the intruder is assumed to be closer to the node which represents the tip of the cone area.
- Intersecting alert links give the most precise estimate of the position and the intruder is within the area delimited by the intersection points.

If the distance between the current position estimate and the previous one is large the current estimate is neglected, otherwise the estimated position of the intruder is updated. To smoothen the estimated trajectory of the intruder, the position estimates are filtered with a moving average.

4.4.3 Evaluation of the intrusion detection monitoring system

To evaluate the performance of the intrusion detection system described in the previous sections, four different testbeds are used. The first testbeds are the two corridors already introduced in section 4.3.2, with 1 and 2 meters nodes interval. The other two testbeds are square type, where on each side of the square an equal number of nodes are placed with 1 and 2 meters nodes interval. The first square testbed covers a 9 m^2 area and the second a 36 m^2 area. The four test beds are shown in Figure 34 (a)-(d), in which also the path followed by the person in the tests is illustrated (dashed line). The estimated positions obtained through the real-time DFL system are represented with dots.

In both corridors the system estimated the trajectory of the intruder correctly. However, it can be observed that at the edges of the monitored area, the position estimates are missing, are sparse, or inaccurate. The reason being that at the borders the alerts received at the sink are scarcer then in situations where the intruder is in the center of the monitored area. For example at the horizontal ends of the corridors, there is only one link monitoring the area. The nodes detect the intrusions and alerts are transmitted to the sink, but the Matlab application neglects the alerts since single alerts are not evaluated as stated in the 1st rule. This



(a)

(b)

(c)

(d)

Figure 34 Approximate path illustrated with the dashed red line and the real-time position estimates shown with blue dots from the four different tests. Black dots in the figures illustrate the positions of the nodes. Testbeds (a) and (c) had a node interval of 1 meter and in testbeds (b) and (d) nodes were placed 2 meters apart from each other. The width of the corridor in both cases was 2 meters.

phenomenon is most visible when the person enters the corridor from the left as illustrated in Figure 34 (b). In this testbed (2 m nodes interval) the area at the horizontal ends of the corridor, where only one link is able to trigger the alerts, is much larger than in the other testbeds. The person isn't detected until the nodes beside the edge links also raise the alerts. In the vertical direction the same phenomenon does not occur since there are multiple links capable of triggering the alerts simultaneously.

The position estimates aren't as accurate on the borders, due to the fact that alerts are not raised by as many links as in the center of the monitored area, but also because the alert links do not intersect one another. When the intersection points as seen in Figure 33 (a) are missing, estimation of the second coordinate becomes challenging. The x-coordinate estimate in the second entrance of test illustrated in Figure 34 (a) is apparently false. The estimated y-coordinate is accurate since there is six nodes locating on the line, but the x-coordinate has to be determined using the 2nd rule. The first position estimate is correct but the second estimate is poor because the link closest to the intruder's actual position doesn't raise the alert as long as the other links. This results that the alert of the closest link is not considered in the second position estimate. Also the sliding average of the position estimates doesn't smoothen the trajectory since there is only one prior position estimate.

Position estimates in the square testbeds follow the trajectory of the intruder correctly and entrances/exits of the intruder are estimated more precisely compared to the corridor testbeds. The reason being that in the square testbeds there are always multiple links to trigger the alerts. At the borders, the sink receives multiple alerts from various links when the intruder enters and exits the monitored area, thus improving the performance of DFL system. The error between the actual and estimated paths cannot be verified since the precise paths were not tracked at the time of the tests, but it can be seen from Figure 34 (c) and (d) that the error is always within half of the nodes interval, i.e. for 1 meter nodes interval the position estimate is within half a meter and for 2 meters nodes interval the position estimate is within a meter.

The accuracy of the position estimates is a result of the relatively narrow sensitivity area of the LoS and the dense mesh of LoS links over the monitored area. The sensitivity area sets the margin for the position estimate to be within 0.25 m from the LoS and if alert links intersect, the point where the two links cross, span a circle with a radius of 0.25 m for the possible location of the intruder. Multiple intersection points improve the estimate even further as the possible area for the intruder's position narrows down.

5 Conclusions

The objective of this thesis was to design, develop and test an embedded algorithm, computed locally in the nodes of a WSN, to detect the presence of a person located inside the monitored area. In addition, the aim was to localize and track the intruder through the aggregated alerts received from the nodes of the network. Within this scope, implementation of an easily configurable, easy-to-use, real-time intrusion detection and tracking system was planned.

In the thesis, a review of current DFL and tracking systems that are based on the RSSI measurements was done to determine a framework for the real-time intrusion detection and tracking system. Within the thesis scope, the aim was to examine the strengths of each system while avoiding the weaknesses, to assure maximal performance for the developed system while considering the limited resources set by the sensor networking platforms.

An important aspect of the work was validating interference produced by coexisting systems and identifying the sources of RSSI variability. To establish this, interference of WLAN was investigated and the influence to the WSNs performance was discussed. Furthermore, two methods to rank the radio channels were proposed in order to maximize the performance of the developed system. The impact of transmission power, nodes distance, and the surrounding environment on RSSI variability were studied in order to determine a framework for the RSSI characteristics.

The development of a real-time intrusion detection and tracking system was presented in this thesis. The proposed system consists of three mutually dependent pieces: the communication procedure of the WSN, the embedded algorithm ran locally in the nodes to detect the presence of an intruder, and localization and tracking of the intruder from the aggregated alerts received at the sink node of the network.

The nodes of the network exploit a high-accuracy TS protocol that enables the nodes to communicate in a TDMA fashion. The TDMA based communication schedule allows the nodes of the network to disable their radio when scheduled communications are not expected, thus leading to an increase in network lifetime. In addition, the network is tolerable to nodes failure since each node locally determines the communication schedule, thus being independent and not required to receive from the other nodes.

The timeline of the application was thoroughly investigated and the duration of the executed operations during the transmission and reception slots were presented. The results exposed the minimum length for the TDMA slot. In addition, the duration of having the radio turned off during run time was revealed.

The embedded algorithm, which is computed locally in the nodes, allows transmitting only significant information related to intrusions in the monitored area to the sink node. The embedded algorithm reduces both the communication overhead of the network but also the required processing by the Matlab application that is used for localizing and tracking the intruder. The need to minimize communication overhead in single-hop star networks (as in this thesis) is not consequential, but it plays an ever more important role when complexity of the network topology is increased.

The effect of a person to a node’s RSSI measurements was investigated and the results were used to develop an embedded algorithm capable of detecting LoS crossings. The algorithms performance was validated and proved to correctly raise the alerts when LoS crossings occur. Also false alerts were detected but they were caused by the imperfect radiation pattern of the omnidirectional antenna and the reflections of radio signals from nearby obstacles.

The combined alerts received at the sink node enable localization and tracking of the intruder. The positioning and the tracking procedure proposed in this thesis exploits the known locations of the nodes and by evaluating the aggregated alerts based on four distinct rules. In addition, to smoothen the estimated trajectory of the intruder, the position estimates were filtered with a moving average.

The performance of the intrusion detection system presented in this thesis was evaluated using four different testbeds. The tests were conducted in the lobby of a university building in an obstacle free environment and the aim was to detect and track a single intruder moving in the area monitored through the WSN. In each testbed the network consisted of 12 nodes and a sink node. In every test, the system was able to correctly estimate the trajectory of the intruder in real-time. The results indicate that accuracy of the system depends not only on the node density of the network, but also on the spatial location of the intruder and the layout of the network. The case where only single links were capable of detecting the intruder, led to situations where position estimation and tracking were clearly worse compared to areas where multiple links were able to raise the alerts simultaneously.

The main objective of this thesis was to design and implement a real-time intrusion detection system that is based on distributed processing of the RSSI. A person moving inside the monitored area causes attenuation of the radio signal, thus enabling the detection of the intruder. The combined alerts from multiple nodes allow locating the intruder accurately and to track the intruders movements in real-time. After all it is justifiable to say that the goals of the thesis were met. Future study on the topic will focus on exploring different tracking filters suitable for the desired needs. In addition, more realistic scenarios will be studied, such as obstructed environments and situations where there are more than one intruder to be localized and tracked. The possible solutions to overcome the problems stated above should be solved in a way that the overall goal of the project is kept in mind. At the end of the day, we want a system that can monitor large areas in real-time requiring a synchronized, multi-hop network capable of localizing and tracking multiple intruders with minimal latency.

6 References

Benkic, K., Malajner, M., Planinsic, P. and Cucej, Z., 2008, “Using RSSI Value for Distance Estimation in Wireless Sensor Networks Based on ZigBee,” Proceedings of the 15th International Conference on Systems, Signals and Image Processing (IWSSIP 2008), pp. 25-28.

Bluetooth, 2010, available at: http://www.bluetooth.com/.

Bocca, M. Cosar, E. I., Salminen, J. and Eriksson, L. M., 2009. “A Reconfigurable Wireless Sensor Network for Structural Health Monitoring”, Proceedings of the 4th International Conference on Structural Health Monitoring on Intelligent Infrastructure (SHMII-4), 9 pp.

Bocca, M., Mahmood, A., Eriksson, L. M., Kullaa, J. and Jäntti, R., 2011, “A Synchronized Wireless Sensor Network for Experimental Modal Analysis in Structural Health Monitoring”, Computer-Aided Civil and Infrastructure Engineering (CACAIE), to appear.

CC2420, 2010, “2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver”, available at: http://focus.ti.com/lit/ds/symlink/cc2420.pdf.

CC2431, 2010, “System-on-Chip for GHz Zigbee / IEEE 802.15.4 with Location Engine”, available at: http://focus.ti.com/lit/ds/symlink/cc2431.pdf

Ceriotti, M., Mottola, L., Picco, G. P., Murphy, A. L., Guna, S., Corra, M., Pozzi, M., Zonta, D. and Zanon, P., 2009, “Monitoring Heritage Buildings with Wireless Sensor Networks: The Torre Aquila Deployment”, Proceedings of the 2009 International Conference on Information Processing in Sensor Networks (IPSN ’09), pp. 277-288.

Chen, Y. and Terzis, A., 2010, “On the Mechanisms and Effects of Calibrating RSSI Measurements for 802.15.4 Radios”, Adjunct Proceedings of the 7th European Conference on Wireless Sensor Networks (EWSN 2010), pp. 256-271.

Cosar, E. I., 2009, “A Wireless Toolkit for Monitoring Applications”, Master’s thesis, Helsinki University of Technology.

Dong, X. and Vuran, M. C., 2010. “Spatio-temporal Soil Moisture Measurement with Wireless Underground Sensor Networks”, Proceedings of the 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net '10), pp. 1-8.

Eriksson, L. M., Elmusrati, M. and Pohjola, M., 2008. ”Introduction to Wireless Automation - Collected Papers of the Spring 2007 Postgraduate Seminar”, Espoo, Finland: Helsinki University of Technology, Department of Automation and Systems Technology, Report 155.

Faheem, A., Virrankoski, R. and Elmusrati, M., 2010, “Improving RSSI Based Distance Estimation for 802.15.4 Wireless Sensor Networks,” Proceedings of the 2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS 2010), pp. 1-4.

FreeRTOS, 2010, “FreeRTOS Implementation Modules”, available at: http://www.freertos.org/implementation/index.html.

Ha, J. Y., Kim, T. H., Park, H. S., Choi, S. and Kwon, W. H., 2007. “An Enhanced CSMA-CA Algorithm for IEEE 802.15.4 LR-WPANs”, IEEE Communications Letters, vol. 11 no. 5, pp.461–463.

HART Foundation, 2010, available at: http://www.hartcomm.org/.

Hasler, A., Talzi, I., Beutel, J., Tschudin, C. and Gruber, S. 2008, “Wireless sensor networks in permafrost research – concept, requirement, implementation and challenges”, Proceedings of the 9th International Conference on Permafrost, pp. 669-674.

Hussain, S., Peters, R. and Silver D. L., 2008. “Using Received Signal Strength Variation for Surveillance in Residential Areas”, SPIE Proceedings on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, vol. 6973, 6973OL, pp. 1-6.

IEEE 802.11, 2010, available at: http://www.ieee802.org/11/.

IEEE 802.15.1, 2010, available at: http://www.ieee802.org/15/pub/TG1.html.

IEEE 802.15.4, 2010, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)”, available at: http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.

Kahn, J. M., Katz, R. H. and Pister, K. S. J., 2000. “Emerging Challenges: Mobile Networking for Smart Dust”, Journal of Communications and Networks, vol. 2, pp. 188-196.

Kumar, A., Manjunath, D. and Kuri, J., 2008. ”Wireless Networking”, 1st edition, Morgan Kaufmann.

Lee, J.-S., Su, Y.-W. and Shen, C.-C., 2007, “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi”, Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007), pp. 46-51.

Leopold, M., Dydensborg, M. B. and Bonnet, P., 2003. “Bluetooth and Sensor Networks: a Reality Check”, Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys ’03), pp. 103-113.

Lin, S., Zhang, J., Zhou, G., Gu, L., He, T. and Stankovic, J. A., 2006. “ATPC: Adaptive Transmission Power Control for Wireless Sensor Networks”, Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys ‘06), pp. 223-236.

Lymberopoulos, D., Lindsey, Q. and Savvides, A., 2006, “An Empirical Characterization of Radio Signal Strength Variability in 3-D IEEE 802.15.4 Networks Using Monopole Antennas”, Proceedings of the Third European Workshop on Wireless Sensor Networks (EWSN 2006), pp. 326-341.

Mahmood, A. and Jäntti, R., 2009, “Time Synchronization Accuracy in Real-Time Sensor Networks”, Proceedings of the 9th IEEE Malaysia International Conference on Communications (MICC 2009), pp. 652-657.

Maróti, M., Kusy, B., Simon, G. and Lédeczi, Á., 2004, ”The Flooding Time Synchronization Protocol”, Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys ’04), pp. 39-49.

Mottola, L., Picco, G. P., Ceriotti, M., Guna, S. and Murphy, A. L., 2010, “Not All Wireless Sensor Networks Are Created Equal: A Comparative Study On Tunnels”, ACM Transaction on Computational Logic, Vol. 7, No. 2, Article No. 15.

MSP430, 2010, “MSP430x1xx Family, User’s Guide”, available at: http://focus.ti.com.cn/cn/lit/ug/slau049f/slau049f.pdf.

Ohrtman, F. and Roeder, K., 2003, “Wi-Fi HandBook, Building 802.11b Wireless Networks”, McGraw-Hill Companies.

Patwari, N. and Wilson, J., 2010, “RF Sensor Networks for Device-Free Localization: Measurements, Models, and Algorithms”, Proceedings of the IEEE, vol. 98, no. 11, pp. 1961-1973.

Petrova, M., Riihijärvi, J., Mahonen, P. and Labella S., 2006, “Performance study of IEEE 802.15.4 using measurements and simulations”, Proceedings of the IEEE Wireless Communications and Networking Conference, 2006. (WCNC 2006), pp. 487-492.

Rappaport, T., 2001. “Wireless Communications: Principles & Practice”, 2nd Edition, Prentice Hall,

RFC1122, 1989, Network Working Group of the IETF, 1989, “Requirements for Internet Hosts – Communication Layers”, available at: http://tools.ietf.org/html/rfc1122

Rom, R. and Sidi, M., 1990, “Multiple Access Protocols: Performance and Analysis”, Springer-Verlag.

Römer, K. and Mattern, F., 2004, ”The Design Space of Wireless Sensor Networks”, IEEE Wireless Communications, vol. 11, no. 6, pp. 54-61.

Sensinode, 2006, “Micro Hardware Manual”.

Sensinode, 2007, “NanoStack Reference”.

Shaterian, K. and Gharaee, H., 2010, “DTFM detection with Goertzel algorithm using FPGA, a resource sharing approach”, Proceedings of the 2010 International Conference on Electronic Devices, Systems and Applications (ICEDSA 2010), pp. 196-199.

Shelby, Z. and Bormann, C., 2009. “6LoWPAN: The Wireless Embedded Internet”, John Wiley & Sons, Inc.

Shuaib, K., Boulmalf, M., Sallabi, F. and Lakas A., 2006, “Co-existance of ZigBee and WLAN, a Performance Study”, Proceedings of the IEEE Wireless Telecommunications Symposium (WTS 2006), pp. 1-6.

Sikora, A. and Groza, V. F., 2005, “Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band”, Proceedings of the IEEE Instrumentation and Measurement Technology Conference 2005 (IMTC 2005), pp.1786-1791.

Siva Ram Murthy, C. and Manoj, B. S., 2004. “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall.

Srbinovska, M., Gavrovski, C. and Dimvec, V., 2008, “Localization Estimation System Using Measurement of RSSI Based on Zigbee Standard,” Proceedings of the 17th International Scientific and Applied Science Conference, pp. 45-50.

Srinivasan, K. and Levis, P., 2006a, “RSSI is Under Appreciated”, Proceedings of the 3rd Workshop on Embedded Networked Sensors (EmNets’06).

Srinivasan, K., Dutta, P., Tavakoli, A. and Levis, P., 2006b. ”Understanding the Causes of Packet Delivery Success and Failure in Dense Wireless Sensor Networks”, Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys ’06), pp. 419-420.

Stallings W., 2004. “Wireless Communications and Networks”, 2nd edition, Pearson Education.

Sugano, M., Kawazoe, T., Ohta, Y. and Murata, M., 2006, “Indoor Localization System using RSSI Measurement of Wireless Sensor Network Based on Zigbee Standard,” Proceedings of the IASTED International Conference on Wireless Sensor Networks, pp. 1-6.

Tang, L., Wang, K.-C., Huang, Y. and Gu, F., 2007, “Channel Characterization and Link Quality Assessment of IEEE 802.15.4-Compliant Radio for Factory Environments,” IEEE Transactions on Industrial Informatics, vol. 3, no. 2, pp. 99-110.

Tuononen, A., 2009, “Wireless Sensor Networks in Condition Monitoring of Electrical Applications”, Master’s thesis, Helsinki University of Technology.

Wikipedia dBm, 2010, available at: http://en.wikipedia.org/wiki/DBm

Wilson, J. and Patwari, N., 2010a, “Radio Tomographic Imaging with Wireless Networks,” IEEE Transactions on Mobile Computing, vol. 9, no. 5, pp. 621-632.

Wilson, J. and Patwari, N., 2010b “See Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks,” IEEE Transactions on Mobile Computing, available at: http://doi.ieeecomputersociety.org/10.1109/TMC.2010.175.

WiMedia Alliance, 2010, available at: http://www.wimedia.org.

Wi-Fi Alliance, 2010, available at: http://www.wi-fi.org/.

Woyach, K., Puccinelli, D. and Haenggi, M., 2006, “Sensorless Sensing in Wireless Networks: Implementation and Measurements,” Proceedings of the Second International Workshop on Wireless Network Measurement (WiNMee 2006).

Yick, J., Mukherjee, B. and Ghosal, D., 2008, “Wireless sensor network survey”, Computer Networks, vol. 52, no. 12, pp. 2292-2330.

Zanca, G., Zorzi, F., Zanella, A. and Zorzi, M., 2008. “Experimental Comparison of RSSI-based Localization Algorithms for Indoor Wireless Sensor Networks”, Proceedings of the Workshop on Real-World Wireless Sensor Networks (REALWSN '08), pp. 1-5.

Zhao, J. and Govindan, R., 2003, “Understanding Packet Delivery in Dense Wireless Sensor Networks”, Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys ‘03), pp. 1-13.

Zhang, H.-X., Lu, Y.-H. and Bao, Y.-F., 2003, “The Study on Fading Characteristics of Outdoor Time-Variant Wireless Channel using FDTD Method”, Proceedings of the 6th International Symposium on Antennas, Propagation and EM Theory (ISAPE ’03), pp. 564-567.

Zhang, D., Ma, J., Chen, Q. and Ni, L. M., 2007, “An RF-Based System for Tracking Transceiver-Free Objects,” Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications, (PerCom’07), pp. 135-144.

Zhang, D. and Ni, L. M., 2009, “Dynamic Clustering for Tracking Multiple Transceiver-Free Objects,” Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications (PerCom’09), pp. 1-8.

ZigBee Alliance, 2010, available at: http://www.zigbee.org/.

ZigBee, 2007, “ZigBee and Wireless Radio Frequency Coexistence”, available at: www.zigbee.org/imwp/download.asp?ContentID=11745