A Patient Identification System using RFID and IEEE 802.11b Wireless Networks

ANTONIO AGUILAR

KTH Information and
Communication Technology

Master of Science Thesis
Stockholm, Sweden 2007

COS/CCS 2007-13

A Patient Identification System using RFID and IEEE 802.11b Wireless Networks

Antonio Aguilar

Examiner: Prof. Gerald Q. Maguire Jr.
Supervisor: Prof. Wil van der Putten

March 23, 2007

Foreword

This work is presented in partial fulfilment of the requirement for the degree of Master in Science at the Department of Communication Systems (CoS), School of Information and Communication Technology (ICT), at the Royal Institute of Technology (KTH), Stockholm, Sweden.

This work was carried out at the Department of Medical Physics and Bioengineering at the University College Hospital Galway, Ireland and the National University of Ireland, Galway.

Abstract

The recent increased focus on patient safety in hospitals has yielded a flood of new technologies and tools seeking to improve the quality of patient care at the point of care. Hospitals are complex institutions by nature, and are constantly challenged to improve the quality of healthcare delivered to patients while trying to reduce the rate of medical errors and improve patient safety. Here a simple mistake such as patient misidentification, specimen misidentification, wrong medication, or wrong blood transfusion can cause the loss of a patient's life. Misidentification of patients is a common problem that many hospitals face on the daily basis. Patient misidentification is one of the leading causes of medical errors and medical malpractice in hospitals and it has been recognised as a serious risk to patient safety.

Recent studies have shown that an increasing number of medical errors are primarily caused by adverse drug events which are caused directly or indirectly by incorrect patient identification. In recognition of the increasing threat to patient safety, it is important for hospitals to prevent these medical errors from happening by adopting a suitable patient identification system that can improve upon current safety procedures.

The focus of this master's thesis is the design, implementation, and evaluation of a handheld-based patient identification system that uses radio frequency identification (RFID) and IEEE 802.11b wireless local area networks to identify patients. In this solution, each patient is given a RFID wristband which contains demographic information (patient ID number, ward number, hospital code, etc.) of the patient. A handheld device equipped with IEEE 802.11b wireless local area network connectivity and a RFID reader is then used by the medical staff to read the patient's wristband, identify the patient, and access the relevant records of this patient.

This work was carried out at the Department of Medical Physics and Bioengineering at the University College Hospital Galway (UCHG), Ireland and the National University of Ireland, Galway.

Sammanfattning

Ökande de nya fokuserar på patientsäkerhet i sjukhus har givit en översvämning av nya teknologier och bearbetar sökande att förbättra det kvalitets av patient omsorg på peka av omsorg. Sjukhus är komplexa institutions vid naturen och utmanas ständig för att förbättra det kvalitets av sjukvården som levereras till prövas patient för att förminska klassa av medicinska fel och för att förbättra patient säkerhet. Här kan ett enkelt fel liksom patient misidentification, specimenmisidentification, fel läkarbehandling eller fel blodtransfusion orsaka förlusten av ett liv för patient. Misidentification av patient är ett allmänningproblem som många sjukhus vänder mot daglig. Patient misidentification är en av leda orsakar av medicinska fel, och den medicinska malpracticen i sjukhus och den har känts igen som ett allvarligt riskerar till patient säkerhet.

Nya studies har visat att ett ökande numrerar av medicinska fel orsakas i första hand av motsatt droghändelser vilka orsakas direkt eller indirekt av oriktigt patient ID. I recognition av den ökande hot till patientsäkerhet är det viktigt att sjukhus förhindrar dessa medicinska fel från att hända, genom att adoptera ett passande patient ID system som kan förbttra på säkerhetsrutin.

Fokusera av denna avhandling är designen, genomförande, och utvärderingen av ett patient IDsystem, som använder radiofrekvensidentifiering (RFID) och radion 802.11b, knyter kontakt för att identifiera patient. I denna lösning ges varje patient ett RFID-armband som innehåller demografikinformation (den patient personnumer, avdelning kod, sjukhuset kod, osv.) av patient. En handdator, som utrustas med trådlös IEEE 802.11b och en RFID-sändare/mottagare, används därefter av den medicinska personal för att läsa armbandet för patient och för att identifiera patient.

Detta arbete bars ut på avdelningen av medicinskfysik och bioteknik på Universitetssjukhuset Galway (UCHG), Irland och den Nationella Universitet av Irland, Galway.

Dedication

To Brendan and Gloria.

Acknowledgements

There are two very important people that I would like to express my gratitude.

I would like to express my most sincere gratitude to my thesis examiner, Prof. Gerald Q. "Chip" Maguire Jr. for his invaluable feedback, help, and patience during the project, and while I worked on this thesis. His advise and comments always pushed me to deliver the highest quality of work, and his views on technology and innovation have greatly influenced my professional life as an electronics engineer.

I am highly indebted to my supervisor Prof. Wil van der Putten for allowing me to be part of his department, for his complete trust, and for providing all the opportunities and facilities to carry out this research project. Without his support and advise, I would not be where I am now.

With my most sincere respect and gratitude, I thank you both for everything you helped me achieve.

Antonio Aguilar.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This master's thesis is the result of a project conducted at the Department of Medical Physics and Bioengineering at the University College Hospital Galway in co-operation with the National University of Ireland, Galway. This thesis is in partial fulfilment of the requirements for the degree of the Master's in Science at the Royal Institute of Technology, Stockholm, Sweden.

1.1 Previous Work

The problem of patient misidentification is a very challenging topic in healthcare. It is recognised that patient misidentification errors occur on a daily basis in many hospitals worldwide. Patient misidentification can lead to all sorts of medical errors and increases the risk to the patient's safety.

Hospitals are complex institutions by nature, with the human interactions between the medical staff and the patients being a crucial element in the timely delivery of care to patients. Physicians and nursing staff interact with thousands of patients per year, providing healthcare services to them. In order to successfully provide these services, physicians and nurses must first correctly identify the patient, as part of a repetitive sequential process of serving this client. Because of the larger number of these human interactions

with patients, human errors may be introduced in the process[1]. One of those common errors is misidentifying a patient.

To describe in greater detail the scope of the patient misidentification problem, consider the following case scenarios:

> "A young lady in her late twenties was going to surgery the next morning. She was on nothing by mouth. Due to error of misidentification, a tray was inadvertently given to the patient on the morning of surgery. Perhaps the patient thought it was okay, so she ate her food and said nothing. Later that morning, she was taken to surgery. During the procedure, she threw up and aspirated her vomits. She had a cardiac arrest and was later revived. It was too late because the sensory nerve damage had occurred. She sustained brain damage and became paralysed. The hospital took good care of her for a couple of years as part of the settlement. One day she was left unattended in the x-ray department while waiting for a procedure, and she was later found dead. Correct identification before issuing a food tray to the patient going to surgery could have prevented the tragedy [74]".

consider this other scenario:

> "In a hurry, a nurse picked up medication for one patient and inadvertently administered it to a wrong patient. In a hurry to do her work, she misidentified the patient supposed to receive the medication. Although the five rights are supposed to help double check medication before it is administered, in a hurry, deviation and shortcuts may occur leading to tragic errors. The right medication for the right patient through the right route, with the right dosage, at the right time is the standard in many

[1]Figures for typical industry process control is 3 sigma (67,000 defects per million), today industry is aiming at 6 sigma (3.4 defects per million) quality control. In this context, if a hospital treats 100,000 patients per year then at 3 sigma there were would be 67 "reportable events", some of these will be minor and some serious.

hospitals. This should help to decrease medication errors [74]".

These two scenarios are from "101 ways to prevent medical errors" by Yinka Vidal [74]. It can be seen from these scenarios and others that the health of the patients was put at risk due to misidentification.

The extent to which patient misidentification occurs within a hospital is usually widely *underestimated* by the medical staff, as very often they may be unaware that a misidentification has occurred. For this reason, misidentification incidents are difficult to track and document as they happen and are rarely reported on a daily basis. Common medical error handling practice in some hospitals typically begins with the so called "shame and blame" method, where physicians are held personally responsible for mistakes. Such damaging, finger pointing approach noticeably discourages error reporting, especially since everything a physician states for the record is subjected to legal findings. Misidentification errors, to a large extent are attributed to the fact that the medical staff becomes complacent on their daily practices or may take "short-cuts" in their patient identification procedures.

Patient misidentification errors can lead to all sorts of serious outcomes for patients. The following types of incidents are possible:

- Administration of the wrong drug to the wrong patient.
- Performance of the wrong procedure on a patient.
- Delays in commencing treatment on the correct patient.
- Patient is given the wrong diagnosis.
- Patient receives inappropriate treatment.
- Wrong patient is brought to operating theatre.
- Cancellation of operations due to the misfiling of results or medical documentation.

As surprising as it may sound, many hospitals worldwide still do not have patient identification systems in place. This is mostly attributed to economic,

management, and educational factors in these organisations. However, some hospitals have already adopted a patient identification scheme of one sort or another; in order to reduce or prevent patient misidentification from happening. The following are some of the different approaches that a hospital may take to address the patient misidentification problem:

Verbal and visual identification: Patients are asked for their names as proof of identity. Also, they may be visually recognised by the medical staff before performing a medical service. However, this approach has problems since in many cases patients may not be able to speak or conscious enough to provide their name. The visual appearance of the patient due to his/her condition may also present an impediment to identify the patient[2].

Chart-based identification: The medical staff uses the patient's medical chart to identify the patient. In hospitals that are strongly paper-based, it is common to find the patient's medical chart[3] beside the patient's bed or near the patient. Before performing a medical service, the medical staff checks the patient ID number and name from the medical chart to identify the patient. However, this approach is prone to errors since a medical chart may be misplaced or wrongly referenced and in the worst case, lost.

Hand-written wristband: This is one of the most common methods used in hospitals. In this approach, the medical staff writes basic information on a plastic or paper-based wristband to identify the patient. This method can be used to complement the chart-based identification. However, this approach has some problems: illegible hand writing, and limited information can be put on the wristband. This approach may also lead to multiple wristbands worn by a patient which may confuse the medical staff and complicate the delivery of healthcare services to the patient.

[2]For example, the patient suffered severe trauma such as a car accident or fire burns and it is not physically recognisable.

[3]A folder with attached sheets of paper which contains the entire medical history of the patient.

Barcode identification: This is the most commonly adopted method by hospitals that can afford the technology. In this approach, barcode wristbands and barcode scanners are used to identify patients. The use of barcode has had a good degree of success in preventing misidentification and medical errors. However, one of the main arguments against barcode is that it can not provide up-to-date information in real-time, once the barcode wristband is printed, i.e. the information on it can not be changed or updated. It is not clear if this is a requirement for patient identification applications, but it is certainly a feature currently found in other item identification technologies such as radio frequency identification (RFID).

Advanced identification technology: New technology developments such as radio frequency identification, Smart Cards, and biometrics are being considered by many hospitals to implement their patient identification schemes. These technologies, when deployed, can provide more advanced services for tracking, billing, and identifying patients.

In addition, the problem of patient misidentification may be approached using non-technical methods (patient safety guidelines and treatment procedures) or using technical solutions (Barcode, RFID, Smart Card) or a combination of both. The non-technical solutions usually involve the definition of patient safety guidelines or hospital risk management procedures that the medical staff must follow, these procedures once adopted can help to reduce the risks and improve safety of patients. At the same time, technical solutions such as barcode and radio frequency identification can provide the means to enforce patient identification procedures and reduce the risk of patient misidentification from happening.

In this thesis, an electronic system is proposed for identifying patients using wireless technology. The system is based on a commercial handheld and a hardware prototype that uses radio frequency identification (RFID) and IEEE 802.11b wireless networks to identify patients. A prototype patient identification system was constructed in order to demonstrate the concept.

1.2 Problem Statement

The University College Hospital Galway (UCHG) is one of the largest healthcare institutions in the west side of Ireland. This hospital, together with the Merlin Park Regional Hospital (MPRH) are part of the Galway Regional Hospitals in Ireland. Together, these two hospitals provide a wide range of medical services to the communities in the area.

Recently, the University College Hospital Galway has undertaken major developments in its hospital infrastructure in terms of bed and theatre capacity, cardiology services, radiology suites, radiotherapy services along with an expanded building infrastructure. At the same time, the hospital has made recent investments in their IT infrastructure, making UCHG one of the most advanced hospitals in the region.

Currently, the hospital has not yet adopted a hospital-wide patient identification system. However, at the time of this writing, several project trials were being conducted to evaluate the use of barcode for patient and specimen identification within the hospital.

The purpose of this thesis project was to develop and demonstrate an alternative system solution to prevent patient misidentification and improve the accuracy of patient information. The proposed system makes use of radio frequency identification (RFID) technology, mobile handhelds, and wireless LAN technology for patient identification and enhancing the availability of relevant patient information to caregivers (the details of this system will be presented in chapters 4, and 5).

The following were the goals for this thesis project:

- Design and implement a handheld patient identification system based on radio frequency identification and wireless networks with the purpose of preventing patient misidentification.
- Construction of a working prototype to demonstrate the concept and benefits of such system to the hospital.
- Implement an interface to the hospital information system in the

hospital to test the prototype with real data.

- Deploy a wireless network within the hospital that would allow the prototype to be tested in a typical scenario.
- Evaluate the resulting system.

1.3 Scope and delimitations

Since the topic of patient misidentification is very broad, this thesis concentrates on the technical aspects of the design, implementation, and evaluation of a patient identification system - while providing only references for further reading concerning the medical background of this topic. Therefore, the information in this thesis is of technical nature and aimed at readers with a background in medical informatics or IT managers working in healthcare institutions.

1.4 Thesis Outline

The thesis consists of the following chapters:

Chapter 2: This chapter gives a general overview of the different technologies that can be used for patient identification applications in hospitals. It briefly compares these systems in terms of the technology used, limitations, and benefits of each approach with respect to positive patient identification at the point of care. This chapter also briefly covers topics on patient safety, patient identifier schemes, patient privacy, from the point of view of patient identification.

Chapter 3: This chapter provides an overview of the use of wireless local area network technology in hospitals. It describes the considerations, applications, and issues, when using wireless networks in medical environments. It also aims to provide the reader with some recommendations for securing, protecting, and reducing possible

interference problems when deploying wireless local area networks in hospitals.

Chapter 4: This chapter describes the design decisions made for the construction of the patient identification prototype. Several technical choices were evaluated in terms of the software and hardware used in the prototype. A description of how the prototype was constructed is also given in this chapter.

Chapter 5: This chapter describes how the patient identification prototype was tested. It describes how the software interface for the prototype was used to identify users/patients. This chapter also comments on the effects and benefits that the prototype could have in the care of patients.

Chapter 6: This chapter outlines the conclusions regarding this thesis work and gives suggestions for future work.

Chapter 2

Patient Identification Systems

This chapter gives a general overview of the different technologies that can be used for patient identification applications in hospitals. It briefly compares these systems in terms of the technology used, limitations, and benefits of each approach with respect to positive patient identification at the point of care[1]. This chapter also briefly covers topics on patient safety, patient identifier schemes, patient privacy, from the point of view of patient identification.

2.1 Patient Safety at the Point of Care

Accurate information about the patient at the point of care is critical to the successful delivery of medication and care to patients in hospitals. In 2001, the U.S. National Institute of Medicine issued an important report titled: "To Err Is Human, Building a Safer Health System", which described the prevalence and widespread problem of medical errors (which are often preventable) throughout hospitals in the United States. The report highlighted that preventable medical errors cause up to 98,000 deaths and

[1]This term refers to the delivery of medical treatment at the actual location where the patient physically resides.

770,000 adverse drug events[2] in the U.S. each year [37]. These are remarkable figures considering that the U.S. has highest expenditure for healthcare of any country in the world [11].

Similar studies in Europe confirm that medical errors are on the increase [44] and subsequent figures published by the U.S. Joint Commission on Accreditation of Healthcare Organisations (JCAHO) have revealed that the problem not only persists, but it appears to be escalating [33].

It was identified in each of these studies, that a large majority of the medical errors were attributed to adverse drug events, specimen misidentification, and incorrect blood transfusions; caused primarily by incorrect identification (direct or indirect) of the receiving individuals [66].

Despite the evidence that medical errors are a persistent and growing problem in many hospitals, very little has been done to reverse the trend [29]. Industry efforts to address patient safety and patient misidentification are mainly focused on error reduction at the point of care usually through technological solutions such as barcode or radio frequency identification [50].

2.2 Overview of Patient Identification Systems

2.2.1 Barcode Identification

A barcode is a machine readable representation of encoded information usually printed on a surface in the form of a pattern[3]. Initially, barcodes could only store limited information in the widths and spacings of printed parallel dark lines (traditional barcode – see figure 2.1) but with recent technology

[2]The term adverse drug event refers to drug administration errors that take a variety of forms including incorrect drug selection, incorrect dosage or frequency, and negative drug interactions.

[3]The idea for the barcode was developed by Norman Joseph Woodland and Bernard Silver in 1948, but it was only in 1962 that it was commercially utilized [56].

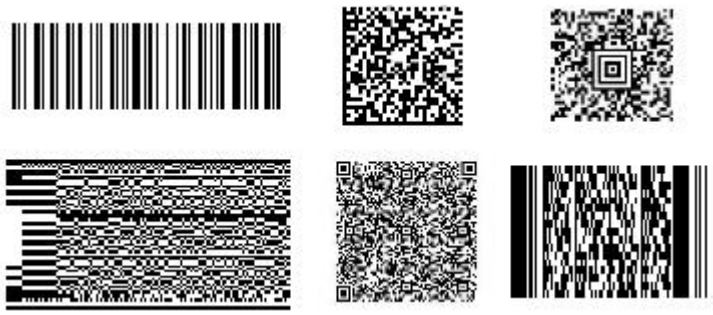

Figure 2.1: Some common barcode encodings.

improvements, barcodes can now be printed in patterns of dots, sequential lines, and two-dimensional images and are able to store up to two-thousand text characters (see figure 2.1).

In healthcare applications, barcode solutions have proven to be effective in reducing patient misidentification, blood transfusion errors, and drug administration errors [2], as part of improving patient safety in hospitals [21].

For instance, in a medication administration application, barcode solutions often include a barcoded wristband issued to the patient at the time of admission (as shown in figure 2.2). Similarly, staff ID badges and medications may also have barcodes printed on them. Usually, when a medication is administered, all the relevant barcodes would be scanned at the bedside, this includes: the patient's barcode wristband, the nurse's ID badge, and the medication's barcode. This assures a match between the patient and the medication, and also identifies the physician or nurse administering the medication for compliance with the "Five rights" of patient medication administration[4] [52].

For patient identification applications, barcodes are primarily used to record demographic information about patients[5]. This barcode information is

[4] *Right* patient, *right* time and frequency of administration, *right* dose, *right* route of administration, *right* drug.

[5] Full names of the patient, date of birth, contact details, civil status, allergies, blood group, etc.

Figure 2.2: Uses of Barcode in healthcare.

usually stored using a barcoded wristband which then serves as an index-key to the patient's medical information on the hospital information system (HIS) or the different clinical systems in the hospital, as shown in figure 2.2[6].

In other clinical applications, hospitals usually deploy barcoding solutions for tagging unlabelled unit-of-use medications, to manage clinical inventory and assets, and to record medical interventions for each patient receiving medications or blood transfusions [20]. Similarly, pharmacies in hospitals use barcoding to update and audit their drug inventory and automate record keeping of pharmaceuticals used in the hospital [35].

2.2.2 Challenges of barcode technology in healthcare

2.2.2.1 Quality of the barcodes and durability

A key requirement of bar coding for healthcare is clarity and definition of the barcode in labels and wristbands. As barcodes become smaller (in order to accommodate more data), the need for readability and precision increases. Edge definition, which refers to the clarity and contrast of the dark and light edges within a barcode symbol, is a problem with ink jet and laser barcode printers and may cause a printed barcode to be prone to misreads. In addition, ink jet and laser printers may require higher quality ink or toner

[6]Images reproduced with permission from PDC Inc.

otherwise there may be undesirable degradation over time in the quality of printed labels and barcodes.

2.2.2.2 Price of the technology

Some hospitals still find barcode technology solutions expensive, since the implications for using barcode in healthcare scenarios usually requires the integration of software, printers, and other barcode equipment with the existing clinical systems at the hospital, and depending on the sophistication of the hospital's IT systems this could be a lengthy, expensive, and complex task.

2.2.2.3 Lack of industry standards and regulations

At present there is no single industry standard regulating the use of barcodes in hospitals and what information should be encoded onto them. In recent years, the U.S. Food and Drug administration has proposed several regulations regarding the use of barcode in American hospitals, but worldwide there are still some significant challenges to the adoption of barcode technologies in healthcare, additionally each hospital usually has different needs. The fact that there are over 200 barcode symbologies and several of them are being considered for use in healthcare applications is an example of this. In addition, it is common to find that medical departments in hospitals have implemented different barcode solutions which are often incompatible with the barcode systems in other departments (e.g. blood bank barcode label is not compatible with laboratory label) this may cause a patient to wear several barcode wristbands or labels[7] at the same time.

[7]Although this particular type of case is rarely reported, nonetheless it exists in many hospitals.

2.2.2.4 Functional limitations of barcode technology

A limitation of barcode is that it can not update information in real-time, once a barcode is printed, the information on it remains fixed and can only be changed by re-printing the barcode. The initial concept of a barcode was intended to operate in this way.

2.2.2.5 Integration and interoperability

A common impediment to the use of barcode technology in hospitals is due to vendor-lock in[8] issue created by companies supplying barcode solutions. Thus if a hospital has already deployed a barcode solution and desires to enhance or change some functionality of their systems using barcode solutions from another vendor, it may prove difficult due to the a single vendor approach and the vendor-lock in of some barcode products. Integration of multiple barcode products is often difficult because the ownership of barcode systems remains in hands of the barcode companies, not the hospitals.

2.2.3 Radio Frequency Identification

The term radio frequency identification (RFID) describes a wireless identification technology that communicates data by using radio waves[9]. Data is encoded in a chip, which is integrated with an antenna and packaged into a finished label or tag, as shown in figure 2.3[10] (a) and (d). RFID tags (also called transponders) may be passive (requiring close proximity to a RFID reader[11]), or active, in which case the RFID tag contains a small battery to allow continuous monitoring (used mostly to track equipment and for long range applications).

[8] A business term used to refer to a created monopoly associated to a single vendor or supplier.

[9] The technology used in RFID has actually been around since the early 1920's.

[10] Images reproduced with permission from PDC Inc.

[11] A RFID reader is a device that can read encoded information from RFID tags or labels.

Figure 2.3: Uses of RFID in healthcare.

RFID technologies offer different rewritability options, memory sizes, and tag forms, and can be read from anywhere within range of the RFID reader. Some RFID labels can hold more data than barcodes, and can be read automatically without any user intervention required.

2.2.3.1 RFID in healthcare applications

At present, the application of RFID technology in hospitals has been modest, mainly due to the cost of the technology. Like most electronic technologies, RFID unit costs have fallen dramatically within the past few years, but have not yet achieved the tipping point of economic viability for cost conscious hospitals. In practical healthcare applications, RFID has been primarily restricted to asset management of documents and medical equipment, patient identification, and other specific applications.

Similar to barcode applications in healthcare, RFID has found intriguing applications for improving the delivery of healthcare and welfare of patients in hospitals. For instance, typical RFID applications in hospitals include:

- Improvement of legacy barcode applications using RFID, i.e. blood transfusion, pharmaceutical tracking, and specimen identification.
- Applications to track long-term care elderly or disoriented patients [48].
- Applications for surgical patients who can be tagged to ensure that the

Figure 2.4: Some commercial RFID readers.

right procedure is being performed on the right person at the right time [67].

- Positive patient identification applications using a smart patient wristband that when scanned by a RFID reader reveals patient name, date of birth, admitting orders, insurance information, surgical site, allergic reactions, medication requirements, and blood type. See figure 2.3 (b) and (c).
- Applications for tracking and monitoring surgical equipment before and after operations [12].
- Applications using implantable RFID devices that act as a portable medical record for patients, see figure 2.3 (e).
- Applications for tracking doctors, nurses, and patients anywhere in a hospital by using RFID enabled badges and ID cards, see figure 2.3 (f).

2.2.3.2 Existing RFID handheld identification systems

Today, there are many RFID readers available in the market for different applications. However, for healthcare applications, features such as: wireless connectivity, barcode support, long battery operation, and multi-tag standard support, must be considered as important requirements.

Figure 2.4[12] shows some of the commercially available RFID readers that can be used for healthcare applications.

- **Precision Dynamics Corporation Feig Tethered Reader R110-00-PDA**

  The R110-00-PDA (as shown in figure 2.4-a) is a tethered 13.56 MHz RFID reader and writer for connection to computers or other data terminals via a RS-232 serial port. This handheld reader is able to identify any transponder simultaneously which follows the ISO-15693 standard[13], e.g. Tag-it, I-Code, my-d, and STM.

- **Precision Dynamics Corporation DR1000 Dual Reader**

  DR1000 Dual Reader (as shown in figure 2.4-b) is a dual RFID and barcode and can read and write to any tags and smart labels compliant with the ISO-15693 industry standard at 13.56 MHz. It provides an easy migration path from barcodes to RFID tags. The reader has no external graphical user interface, but this functionality can be provided by a desktop PC, laptop, or PDA using a RS-232 serial port.

- **Precision Dynamics Corporation TEK RFID Reader P103-00-PDA**

  The TEK P103-00-PDA RFID Reader/Writer (as shown in figure 2.4-c) includes a Palm i705 personal digital assistant device to read and write information to RFID wristbands and labels using an operating frequency of 13.56 MHz . The reader is ISO 15693-1, 2, and 3 compatible and includes a demo program for RFID wristbands.

- **Symbol Technologies MC9000-G RFID Reader**

  The MC9000-G RFID Reader from Symbol Technologies (as shown in figure 2.4-d) is a ruggedized mobile computer that features integrated support for the most popular radio frequency identification standards. This device combines RFID and barcode reading and also has IEEE

[12]Images reproduced with permission from PDC Inc, Symbol Technologies, Socket Communications, and Cathexis Innovations.

[13]Detailed overview of the different RFID standards is outside the scope of this thesis.

802.11b wireless network connectivity, along with a full 1/4 VGA screen and alphanumeric keypad. The software interface for the reader is based on the Windows Mobile 2003 operating system.

- **Socket Communications Compact Flash RFID Reader Card 6E**

  This Compact Flash RFID reader from Socket Communications (see figure 2.4-e) reads and writes to any ISO-15693 and other proprietary 13.56Mhz RFID tags. The reader can be used for asset tracking, access control, and process control – in healthcare, medical, and pharmaceutical applications. This reader has the advantage that it can interface to any commercial handheld equipped with a compact flash connector. The reader comes with an easy to use software wedge interface for scanning RFID tags.

- **Cathexis Innovations Bluetooth RFID reader**

  This light weight RFID bluetooth reader from Cathexis Innovations (see figure 2.4-f), features RFID functionality along with Bluetooth connectivity. The reader aims to replace the typical bulky and cumbersome RFID readers that may not be suitable for medical personnel to carry around. The Bluetooth connectivity of the reader allows it to share RFID tag information with other systems, e.g. Bluetooth equipped handhelds, desktops, and laptops, allowing the reader to be de-coupled from a particular hardware and software implementation. This type of reader may be particularly advantageous in hospitals where the staff already carry PDAs with Bluetooth and WLAN interfaces.

For a more detailed overview of the features and applications of the RFID readers, see [59].

2.2.4 Comparison of Barcode and RFID

The use of RFID technology can substitute barcode solutions in hospitals, but its use so far has been limited to applications where the use of barcode technology is not adequate, e.g. patient tracking applications. RFID overcomes some of the limitations of barcode technology, but at some cost. Table 2.1 illustrates some of the differences between barcode technology and radio frequency identification technology.

It is likely that in the future, barcode solutions and RFID will complement each other in terms of functionality, cost, and usability. Today, hospitals are reluctant to abandon their initial investments in barcode systems simply to introduce technology replacements. As RFID technology matures, the use of RFID will continue to grow in healthcare, particularly via asset and inventory management applications, then it will move towards personnel and patient identification, and tracking of clinical devices and pharmaceuticals.

2.2.5 Challenges of RFID technology in healthcare

2.2.5.1 Quality of RFID tags and reliability

For positive patient identification applications in hospitals, RFID technology inherits some of the challanges of barcode technology. However, there are some differences in terms of reliability of the technologies. For instance, barcode labels are generally reliable (with some rare exceptions) to read while RFID tags currently are not always reliable and will not work with some products or in certain situations. Therefore to avoid these pitfalls, hospitals will most likely continue to use barcode labeling indefinitely as a fallback when RFID fails, e.g. a barcoded tag using the patient name and ID.

Table 2.1: Barcode and RFID technology comparison

Barcode Technology	**RFID Technology**
Barcodes are scanned one at a time. This may present a challenge when a large number of items are to be counted or tracked, e.g. pharmaceuticals, or stacks of documents.	Depending on technology used, up to several hundred RFID tags can be scanned continuously by one RFID reader. This functionality is useful for tracking applications, e.g. documents, medical equipment, and patients.
Once printed, a barcode cannot be modified. In a medical scenario, this means every time new information needs to be included, the barcode labels or wristbands need to be reprinted.	Re-writeable functionality. Most of the short-range, passive RFID tags allow information to be modified. They can potentially be written multiple times, have higher capacity, and can be combined with sensors. Typical capability is 100,000 write operations with a 10 years data-retention life-span.
Requires line-of-sight. This is generally considered a disadvantage in industry applications. However, it can actually be an advantage in healthcare applications where precise identification is required.	No line-of-sight required. This tends to be an advantage in applications that aim to eliminate human intervention, e.g. asset management and tracking applications.
Privacy and security issues. Although the data encoded on the barcode could be encrypted, there is no protection to prevent the barcode data from being copied and decrypted using commercial tools [72].	Similarly, RFID also presents some privacy and security issues. RFID tags allow more sophisticated forms of data protection and encryption than barcode.
Typically cheaper than RFID tags, even in high volumes.	More expensive than barcode printing. The cost of RFID tags can be a disadvantage for cost conscious hospitals.

2.2.5.2 Price of the technology

Price of the technology is the biggest obstacle for using RFID in healthcare. At present, RFID systems cost more to implement and utilize than any barcode system available on the market [3], this is mainly due to the high manufacturing cost of the tags and the reliance upon very few RFID vendors. Although the costs for RFID readers and tags almost seem to match to that of a barcode systems, pricing models of RFID products still remain unclear to many healthcare organisations [64].

2.2.5.3 Lack of industry standards for RFID in healthcare

RFID also suffers from a lack of industry standards. Although ISO and the EPC have produced a comprehensive set of standards for RFID applications in several industries, there is a lack of standards or guidelines for using RFID in healthcare applications. This is due to the controversial privacy implications that RFID technology is facing and the potential violations of security with existing RFID products. An illustration of this ongoing debate is whether RFID can be used as implantable device in humans in hospitals [49].

2.2.5.4 Functional limitations of RFID technology

In healthcare applications, the idea that RFID does not need a line-of-sight between the tag and the RFID reader is incorrect. For example, in typical patient identification scenarios, the RFID tags (wristbands) must be facing the RFID reader, and a direct line must exist between the tag and reader, unobstructed by any metallic or liquid object, or other tags.

In addition, there are functional limitations of passive RFID tags since these tags must absorb enough power from the reader to transmit the stored tag data. In order to accomplish this, the tags must use directional antennas large enough to intercept the needed power from the reader. The need for passive tags to be powered by the RFID reader's radiation pattern further

limits the distance between tag and reader. The amount of reader radiation is also limited by the need to avoid interference with adjacent RFID readers as well as restrictions placed by the U.S. Federal Communications Commission (or similar national regulators) upon human exposure to electromagnetic emissions.

2.2.6 Privacy in RFID

Since the adoption of RFID in the industry there has been a increasing concern on the privacy implications of using the technology. In the retail sector there are several interest groups working towards implementing standards or recommended procedures for using RFID tags and labels. However, there has been insufficient literature available on the implications that RFID has on personal privacy, especially when the technology is used in a medical setting.

In a medical setting one can immediately see the potential of RFID technology for patient tracking and data management, simplifying the interaction with patient data and identification. As a practical baseline, a RFID tag or wristband may be only provided when the patient is admitted to the hospital, the activation of the RFID wristband may be done by the hospital's administrative staff, e.g. in the inpatient clinic or admissions. The RFID wristband therefore will remain active only during the patient stay in the hospital, once the patient is discharged, the RFID must be deactivated[14] and thrown away to prevent the re-use of the wristband.

Another important aspect that must be addressed when using RFID for medical purposes is the way data is stored in the RFID chip. For example, patient data may be stored in a "transparent" format or in encrypted form, the second method provides greater privacy and data protection when the hospital's administrative staff fail to deactivate the tag[15]. Another aspect

[14]This involves erasing the data on the wristband or deactivating the chip. Many RFID chips already have the functionality to do both.

[15]It is a common scenario for some hospitals to let the patient leave the hospital without

to consider is what type of data should actually be stored in the tag, and how and when this information should be used. Current RFID chips have up to 512 kilobytes of storage, enough to store patient demographics and other relevant patient information. This means RFID tags could store patient monitoring and real-time data such as the current medication, laboratory results, allergies, type of treatment, and other biomedical parameters needed by physicians.

2.2.7 Biometric Identification

Biometric technology, in the form of voice, face, iris, and fingerprint recognition has made major improvements in terms of technology in the last ten years and it has been gradually adapted to healthcare processes and applications. Currently, the use of biometrics in hospitals has been limited to the use of voice and fingerprint recognition applications, with the second being the most accepted application [4].

Common applications and benefits of using biometric fingerprint technology in hospitals include:

- **Unique identification of patients across different domains**

  A biometric fingerprint (the generic version of biometric data from any source) can improve identification, retrieval, and access to patient related medical information from the different clinical systems and databases in instances where there is more than one patient identifier numbering scheme used by the hospital[16]. It is a common scenario that once a patient is admitted into the hospital the patient is assigned an internal number (hospital code, bed and ward number, etc.) for use within the hospital for tracking purposes. The use of biometrics can

being properly discharged. Another scenario is when the patient decides to leave the hospital on his/her own will.

[16]Some hospitals use the patient's Social Security Number, medical card number, or insurance number. The different clinical systems must be able to recognise at least one of them.

reduce the overhead of key-indexing the patient in the different clinical systems and databases [51].

- **Simplified patient admission**

  Fingerprint verification can be useful by hospital admissions to identify the patient when they arrive at the hospital and to improve service response, as often, patients may not initially remember their personal details, e.g. medical card number, social security number, insurance number, etc. or may not have this information available with them when they arrive at the hospital.

- **Speed access to medical records and authorization control**

  In the United States due to HIPAA regulations, when a physician needs to consult diagnostic information regarding a patient with another physician than the one treating the patient and requires access to the patient's medical record, the patient has to personally authorize the transfer of their medical records to allow other specialists to view their medical record. Usually, this procedure is done through a single paper form submitted to the patient for signing. With biometrics, the authorization of this procedure can be done electronically and faster, while reducing paper work.

- **Identification of unconscious or impaired patients**

  Biometrics are useful in cases when patients arrive at the hospital in an unconscious state, e.g. after a trauma accident or in a coma, and when their personal details are unknown or can not be obtained[17]. In a similar manner, biometric fingerprints can be used to identify impaired patients such as blind, mute, autistic, or mentally ill patients.

- **Biometric Signature Systems**

  Biometric fingerprinting can be used to simplify the signing of documents by medical personnel. Usually, physicians and nurses are overwhelmed with the time required to sign all of the medical doc-

[17]The patient will have to be register at the hospital prior their admission.

Figure 2.5: Smart Card identification technologies

uments, e.g. forms, reports, laboratory orders, procedures, discharges, etc. to certify and authorize medical services. Delays in signing such documentation can often cause further delays in patient treatment and medication. By using biometrics along with electronic forms, the overhead involved in document signing administration can be reduced.

The future of biometric systems in healthcare still remains an elusive option for many hospitals, as several privacy implications around biometric systems have yet to be clarified, but as the technology matures and user resistance to the technology decreases, hospitals will gradually adopt biometrics to solve identification problems.

2.2.8 Smart Card Identification

A Smart Card is an identification card with an embedded computer chip[18]. Smart Cards have been around for over 30 years, but is only recently that the technology has matured enough to be suitable for use in healthcare applications [8]. A typical Smart Card can provide both portable data storage and cryptographic capabilities for protecting the sensitive medical records of

[18]The microprocessor has memory that stores data in encrypted format. Smart Cards were invented and patented in the 1970s. Their first mass usage was as payment in payphones in France starting from 1983.

patients.

The future of Smart Card identification technology has been viewed as being very promising in healthcare. In Europe, it is estimated that many European states will adopt Smart Card technology as part of their national health programmes[19], e.g. medical cards for use in hospitals [14].

Common applications of Smart Card technology in hospitals include:

- **Personnel and Patient Identification Systems**

  Smart Cards may be used in a hospital for personnel or patient identification purposes (as shown in figure 2.5[20]). The use of Smart Cards becomes important when the medical staff needs authorization and approval to perform a medical procedure or service, e.g. medication administration, access to medical records, ward transfer, update medical records, etc. For patient identification purposes, Smart Card readers may be used at the patient's bedside to identify the patient. Modern patient entertainment systems currently use this method for identifying the patient and for tracking billing information on the services (telephone calls, internet access, films, games, cable TV) that the patient requests during their stay at the hospital [63].

  In addition, Smart Cards can be combined with biometric fingerprint systems to provide a two-factor identification system, as shown in figure 2.5.

- **Electronic Patient Record (EPR) Systems**

  The use of Smart Cards as portable electronic patient records offers many benefits for improving the way healthcare is delivered to patients. For example, common events such as referrals from a primary care physician, to a specialist, usually involve the exchange of the patients

[19]The NETC@RDS project aims to introduce an European Health Insurance Smart Card as a replacement to the E111 form to provide cross-border healthcare insurance information in European member states [62].

[20]Images reproduced with permission from Precise Biometrics Technologies.

most recent medical records from one place to another[21]. By using Smart Cards the overhead in exchanging this medical information can be reduced while improving the efficiency of the transferring of the patient's medical records between physicians.

In a similar manner, using Smart Cards can be a valuable asset for patients with complex medical histories or with strict drug regimens that must rely on unfamiliar healthcare providers during trips and vacations [17]. By using Smart Cards, patients can carry a basic set of health information with them, and in cases of an emergency, the patients would benefit from a portable record that could provide basic information regarding their medications, allergies, organ donor status, emergency contact numbers, prenatal information, and personal insurance data.

However, there are still some limitations that Smart Card technology must overcome in order to be used successfully for portable medical records in healthcare. Currently, Smart Card technology provides limited storage capacity (up to 256-kilobyte memory) in comparison to other storage technologies such as flash memory card, and USB drives with capacities of a gigabyte or more. Also, there are some reliability issues related to Smart Cards, since they could be bent and easy broken and in some instances the Smart Card data might be difficult to retrieve by the Smart Card readers [9].

2.3 Patient identifiers and numbering schemes

While there is no defined numbering standard for patient identification in Europe, the U.S. Joint Commission on Accreditation of Healthcare Organisations (JCAHO) has proposed several guidelines to improve the accuracy of patient identification in hospitals [34].

[21] In the United States, this is done through HIPAA regulations. In other countries, this often proves to be a difficult feat and involves extensive administrative work from the practitioners sides.

As a recommendation, patient identifier numbers should be used instead of names to prevent any misidentification with already existing patient names [40]. Numbers are unique in nature, whereas names are not. In practice, the medical personnel at the hospital will use both at some point [30].

Identification of patients in a hospital usually involves the request of a "personal number" or a medical ID number[22]. Such number is usually linked to a hospital internal number[23], which in turn will be used by the different clinics and departments across the hospital and during the stay of the patient at the institution. Patients on several occasions will be asked to present a "Medical ID Card" as proof of identity, i.e. when patient is received at the Emergency Room[24] or transferred between clinics. However, this procedures vary from hospital to hospital.

More advanced identification and access control mechanisms such as biometrics can be used to provide access control and proof of identity to patients. A typical example of this would be when a patient is to be discharged from the hospital. A fingerprint can be used as proof of identification, authorisation, and consent for when the patient is discharged from the hospital ward.

2.4 Using handheld devices in hospitals

Handhelds are being used for many purposes in healthcare including patient tracking, e-prescribing, education of healthcare professionals, note capture and documentation, monitoring of a patient's vital signs, storage and retrieval of medical reference material, patient chart information, and more recently patient identification. Despite the fast acceptance of handhelds in hospitals,

[22]In some countries this is known as the "Health Insurance Number" often provided by private insurance companies or the country's healthcare system.

[23]It is expected that a patient may receive treatment in different hospitals due to the preference of medical facilities, a hospital code is usually added to back-trace where the patient has received treatment.

[24]In Ireland this is known as the Accidents and Emergencies (A&E) or casualties entrance.

there are still some challenges and limitations that the technology must overcome.

2.4.1 Resistance to change

The need for overcoming resistance to change by the medical staff is crucial to the acceptance of the technology in hospitals. Often the medical staff will not be persuaded to change their working habits unless such changes can show significant benefits to their work [19]. While hospitals might be interested in reducing the different types of medical errors (misidentification, wrong prescriptions and procedures, etc.) that occur on daily basis by using mobile handhelds, the medical staff might feel pressured or fail to understand how this will benefit them [5].

2.4.2 Privacy, security, and data protection on handhelds

Handheld devices are usually small and portable in comparison to a desktop computer or a Tablet PC[25], it is this form factor that makes handheld devices *attractive* to healthcare professionals. However, because of their size, a handheld may present some security and privacy issues as it can be easily lost or stolen and in the worst case damaged. Though a handheld device can be replaced, the sensitive patient data may not be that easily recovered (if such data was stored in the device) or can be accessed by unauthorised individuals, which in turn will present a serious compromise of the privacy of the patient. Therefore, it is recommended that patient sensitive data should not be stored on handheld devices to prevent all the problems described above. If there is a need to store patient information, one must ensure that the data is protected by some mechanism. Current alternatives for data protection are: password protected data, data encryption, and biometrics. The first two are commonly adopted methods in the industry and provide data protection and privacy

[25]A Tablet PC is a portable device usually the size of an A4 sheet, but genarally several centimeters think. Due to its physical dimensions, it is considered bulky and heavy to carry around by medical personnel.

to some extent. However, the third method, biometrics provides a higher level of security and data privacy [58]. Already, fingerprint authentication is available on some handheld models. For example, the HP iPAQ h5555 and the HP iPAQ hx2700 have a built-in biometrics sensor which allows a user to scan their fingers [28], the biometric sensor does this by converting the fingerprint image to a random "map" that is impossible to duplicate [65]. By using biometrics, in the form of fingerprint identification and authentication some of the privacy and security concerns are eliminated.

2.4.3 Operational time and power consumption

Limited operational time and short battery life are currently *the major arguments against* using handhelds devices in task intensive applications. If mobile handheld devices are to be used for daily clinical practice, the current limited operating time must be overcome. For example, operational time for current handheld devices is limited to few hours[26], in addition if the device is connected to a wireless network operational time is reduced. If encryption is used on the network, i.e. VPN or IPSec, then the operational time is reduced even more.

2.4.4 Usability of the devices

One of the most common challenges for handheld devices when used in medical settings is making the systems easy enough to use to significantly reduce the time that medical staff needs to learn the systems, hence enabling them to rapidly benefit from using the new systems. Medical staff are usually overwhelmed with tasks and responsibilities, thus they typically have little time outside their patient care activities to dedicate to learn new skills or

[26]Actual operating time depends on each device and how it is used. Typical times are on average 3 hours while in active mode and a maximum of 6 to 10 hours while in idle mode. However, these times may be reduced if the device is continuously connected to a Bluetooth or WiFi network.

new systems – although most have a requirement for continuing education. Even if some healthcare professionals would like to introduce new systems and improve their practices, they may not find the time to do it. Therefore, the technology or systems to be implemented for a medical setting must be easy to use and learn or must be required by legal or economic reasons.

2.4.5 Not enough studies on the benefits of handhelds

It is important to note that few empirical studies have been conducted on the benefits that handhelds can bring to a particular healthcare organisation [76]. There have been a lot of trials and discussion of the use of handhelds in healthcare, with the common perception that handheld devices will offer benefits to hospitals by improving the efficiency of healthcare provided to patients; however, there is not enough proof that using handhelds actually improves the welfare of the patient. This problem is due to the fact that handheld technology was developed as a niche market for business executives which made the technology expensive. Areas where handhelds are proving to be effective for healthcare organisations are: form filling, task organising, medical reference, drug prescribing, note taking and recording, and other miscellaneous tasks[27]. The combination of all these tasks, if properly managed and conducted may influence the quality of the delivery of healthcare to patients, which some researchers claim will in turn improve the welfare of the patient [86], however not enough studies have been conducted to support this. Although handhelds were originally designed for business and management purposes the technology is slowly being adapting to the needs of healthcare organisations.

2.4.6 Investment in new technology

Since there is limited data available to support the claim that handhelds improve patient care or staff satisfaction, it is difficult to persuade hospitals to invest in the technology since hospitals usually demand substantial return

[27]E-mail, Internet browsing, chat, document viewing, presentations, etc.

on their investments in new systems. Costs for deploying the technology in a hospital will include the handheld hardware, software licenses, and additional networking equipment expenses. In addition, the price of handheld technology is still beyond the budget of some hospitals, the market cost of a typical handheld with basic connectivity features (Infrared or Bluetooth) is around $200 U.S. dollars, while the cost for a handheld with advanced connectivity features such as IEEE 802.11b/g (WLAN) and GPRS be $400 to $600 U.S. dollars. This relatively high cost of handheld equipment has discouraged and delayed hospitals from investing in the technology. At present, the use of handhelds in hospitals is being pursued by medical professionals that are early adopters[28] of mobile devices and use them in their work settings. As more medical professionals begin to use them in their daily practice, the hospitals where they work will take notice and begin to face the issues of funding, official adoption, technical support, networking support, etc. Thus, promoting a more wide adoption of handhelds in hospitals.

2.4.7 Visual limitations of the devices

The limited visual capabilities such as the small screen, icons, and menus are the first thing that new handheld users notice. As they become familiar with the technology they begin to enjoy the bright and colourful displays of the handhelds despite their small screen. Whether the small screen size presents practical problems to a physician depends on what the handheld is being used for. For instance, handhelds are known to be suitable for e-prescribing since the physician can easily tap on drop-down menus and selection boxes of available drugs, and electronically submit the medical prescription. In contrast, current handheld models have limited display capabilities for displaying detailed graphical data, anatomic illustrations, and medical images. This is due to the limited size of the screens and the deficiencies of the current screen technology for displaying high resolution medical images. Of course it should be pointed out that for diagnostic

[28] A marketing term used to refer to enthusiastic people that adopt new technologies as they come to the market.

purposes, even most desktop computer displays do not have sufficient resolution for many diagnostics image tasks.

In addition, an article published by the medical economics archive [45] notes that the small screens on handhelds are insufficient to display the vast amount of patient data the appears on an typical EHR (Electronic Healthcare Record) and that at the same time the usefulness for taking an adequate history of the EHR is limited. However, these limitations will be easily overcome by using Tablet PC computers and the new technological advances in screen technology [22], heads-up displays, and text-to-speech interfaces that are likely to be used with future handheld models.

Chapter 3

Wireless Networks in Hospitals

This chapter provides an overview of the use of wireless LAN technology in hospitals. It describes the considerations, applications, and issues, when using wireless networks in medical environments. It should also provide the reader with some recommendations for securing, protecting, and reducing possible interference problems when deploying wireless networks in hospitals.

3.1 Using wireless networks in hospitals

Hospitals are compelling places to install wireless networks[1], since physicians and nurses usually require a great deal of mobility and timely access to clinical information about patients from several locations within a hospital. In this environment, a wireless local area network (WLAN) can provide many benefits for the delivery of healthcare. Using wireless LANs in a medical environment can greatly improve the productivity of care providers and the accuracy of diagnoses and treatment by facilitating the retrieval of patient related clinical information by physicians [54].

[1]Throughout this chapter, the terms: wireless, wireless networks, and wireless LANs (WLANs) will be used to refer to the IEEE 802.11 wireless technology standard.

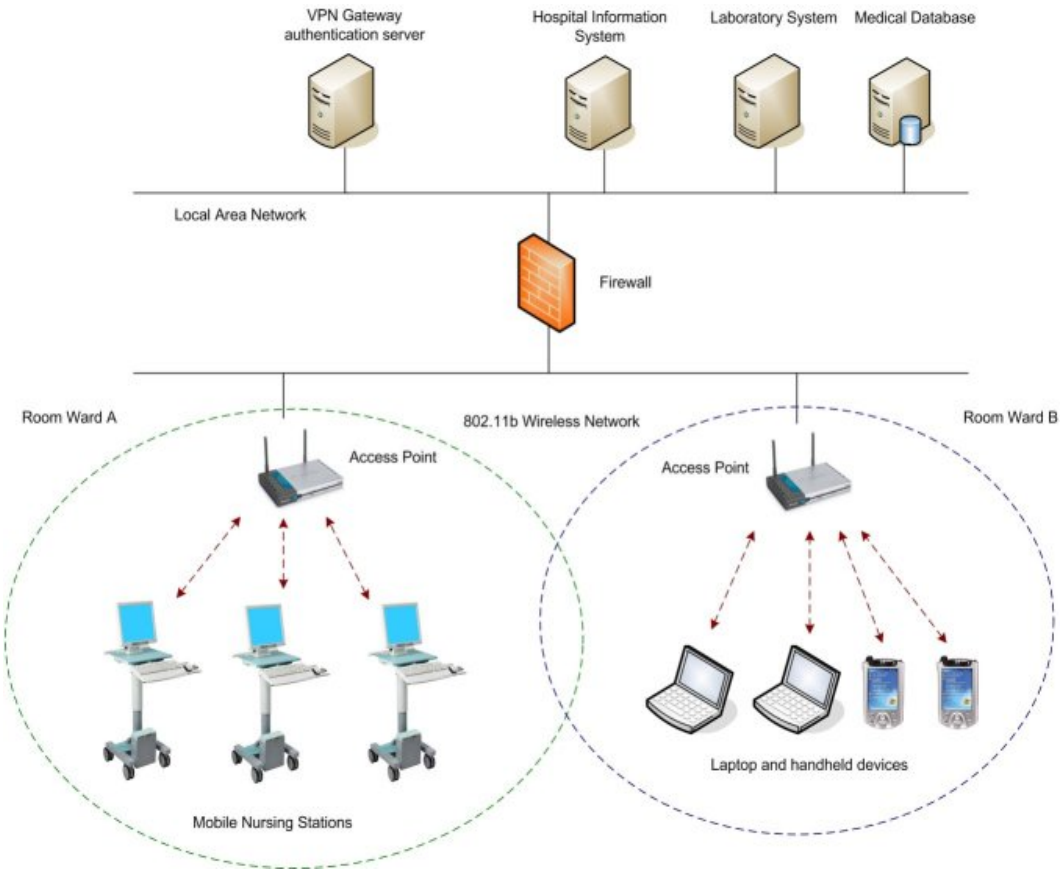

Figure 3.1: A typical deployment of a wireless LAN in a hospital.

The use of wireless networks, combined with the use of clinical information systems, adequate training of medical personnel, IT and network support, and the use of wireless handheld devices could improve the quality and delivery of healthcare in hospitals. Furthermore, the use of wireless networks may also provide a support infrastructure for critically understaffed hospitals, by providing connectivity and access to information in areas where it was not possible before.

Locations where wireless networks could improve operational efficiency and convenience in hospitals usually include high patient traffic areas, such as emergency rooms, critical care wards, nursing stations, doctor's offices, recreational areas, and waiting areas [25].

Today, many hospitals worldwide are deploying wireless networks in their facilities to provide better continuity of care to patients and help improve efficiency and services which the medical personnel depends upon. These features, have contributed to the acceptance of the technology in healthcare [69]. A diagram of a typical deployment of a wireless LAN in a hospital is shown in figure 3.1.

3.1.1 Applications of wireless networks in hospitals

In the last decade, hospitals have valued and recognised the use of wireless technology as a enabling technology for supporting healthcare processes[2]. Since the initial adoption of wireless LAN technology in hospitals back in the mid-1990s, the number and type of applications where wireless LANs have been deployed has grown significantly [10]. Today, hospitals may use wireless LAN technology for the following purposes:

3.1.1.1 Patient charting and prescription management

A wireless LAN, combined with wireless handheld devices can allow caregivers to input and retrieve of health information concerning patients at the point of care, which in turn may help to reduce transcription and prescription errors. Access to such timely information may also facilitate access to adverse drug interactions and medications, patient-specific dose checking, and access to accurate information from the latest medical reference guides.

3.1.1.2 Mobile workstations

In addition to the use of wireless handheld devices, some hospitals have considered the use of wireless mobile workstations to allow caregivers the

[2]Back in 1950 when the first wireless pager was used as tool for physician communication, it was recognised that a wireless device helped to improve the efficiency of physicians on call [60].

ability to collect patient information at the point of care, as well as to enter documentation into the patient's electronic medical record, and place orders for equipment or possible therapies (as shown in figure 3.1). The advantages of a nurse walking from patient to patient collecting and transmitting data via a mobile unit are visible compared to running back and forth to the nursing station for manual input and retrieval of data. Whether these workstations are installed in patient wards or fixed to a rolling cart, wireless LAN technologies may help to facilitate healthcare procedures.

3.1.1.3 Patient registration and identification

The deployment of wireless LANs could help to simplify the process of patient registration through self administered check-in points, e.g. wireless kiosks in hospitals and clinics, either through Smart Card, RFID, or barcode identification. This application can be particularly helpful in under-staffed walk-in health clinics as it could help improve the management of patients and staff resources.

3.1.1.4 On demand communication

In addition to mobile workstations and handheld devices, some hospitals are currently experimenting with voice over IP and presence technology to track and find the closest and most appropriate caregiver on call, without having to depend on one-way paging [32].

3.1.2 Issues when using wireless networks in hospitals

Hospitals may be suitable places to install wireless networks; however, there are many issues to consider before deploying the technology. In terms of technology adoption and implementation, hospitals usually have a set of requirements that must be fulfilled in order to deploy the technology successfully. The following are the main ones to consider:

3.1.2.1 Privacy of medical information

The need for protecting the privacy of patient and clinical information is the principal concern for the deployment of wireless networks in hospitals [73]. This concern is usually fuelled by the perceived weaknesses and vulnerabilities that have been found in wireless networks in recent years [6].

Assuring the privacy of clinical information is a key issue in the design of networked healthcare information systems, as hospitals must comply with strict privacy and data protection regulations, such as HIPAA in the United States [18], the EC 95/46 Directive in Europe [13], or the HPB 517 law in Japan [46]. As an important requirement, hospitals must ensure that the privacy of the patient is not compromised when exchanging clinical information between computer systems, physicians, and other third-party applications.

The use of wireless networks could be a potential privacy risk to hospitals because of possible security breaches that can be exploited if the technology is not properly configured and secured. If the security of the wireless network is compromised it could present a tremendous problem since it could leave both the wireless and wired network exposed and vulnerable to intruders, which in turn could compromises the privacy of the clinical systems in a hospital. Even though electronic patient records provide important information for the medical personnel and the patients, there is a potential for personal harm if disclosed inappropriately. Since clinical information about a patient may be distributed to multiple users within the hospital, it is important to ensure that the information is protected, secured, encrypted, and that authorization and authentication mechanisms are implemented in order to prevent external access this clinical information to unwanted people [27].

3.1.2.2 Network maintenance and IT support

Managing a wireless network and a large number of wireless devices can significantly affect the organisation and efficiency of a hospital's internal IT department. Depending on the architecture of the wireless infrastructure

and the software solutions deployed, procedures should be documented for software distribution and upgrades, device replacements, handling lost or stolen devices effectively, securing data and backup, and virus protection.

In terms of maintenance and IT support responsibility, the most important challenges for deploying a wireless network is in the distribution, maintenance, and configuration of the client software for the wireless stations (this may include software to secure the network, e.g. using WEP/WPA or VPN/RADIUS clients) as this could take several months for a relatively large hospital. As more users in the hospital begin to connect and depend on the wireless network to carry out their daily tasks, maintenance and support for the infrastructure and its users increases, along with increased costs for keeping the network operational. It is this cost aspect of managing wireless networks that has discourage some hospitals from investing in the technology. Nonetheless, depending on the budget, most of this work can be sub-contracted to third-party integrators, which can offer added benefits in terms of network support and technology investment [7].

3.1.2.3 Complex building topologies

A large majority of hospitals are based on conservative or old building topologies e.g. T, L, U, or H shaped building configurations. Commonly, older buildings using these topologies often use concrete or metal building materials which may be obstructive to a wireless transmissions and affect the propagation and coverage of the wireless LAN. Furthermore, most wireless access points typically radiate in a 360 degree pattern around the device to provide a "hot spot" for other wireless devices. In terms of wireless LAN coverage, long narrow corridors in hospitals, will present a challenge for providing efficient wireless network coverage[3]. Thus, it is usually found that when deploying a wireless network in such scenario, detailed RF site surveys need to be conducted to plan ahead for possible coverage and propagation problems that may arise in both small and large hospitals.

[3]Alternative solutions include the use of high directivity antennas and the use of wireless switches.

3.1.2.4 Wireless interference

The proper understanding of radio and electromagnetic interference issues that may arise in hospitals is a crucial requirement for the safe and successful implementation of a hospital wireless network.

Although there is no evidence that IEEE 802.11b/g wireless networks could cause a significant interference problem between wireless devices and medical equipment [68], performing detailed RF surveys early and implementing interference mitigation guidelines will help to minimize any risk. This may include basic testing of critical and life support medical equipment to identify any interference issues and taking measures to provide minimal separation distance from sensitive equipment. Usually, these tests must be performed by the hospital's bioengineering department in co-operation with the IT department to ensure that any possible risks can be managed.

3.2 Wireless network security in hospitals

3.2.1 Security concerns with IEEE 802.11 networks

Unlike wired systems, which can be physically secured, wireless networks are not confined to the inside of buildings. They can be detected as far as 100 meters outside of the premises using a laptop and a directional antenna. This makes wireless local area networks inherently vulnerable to interception and network hacking.

Thus, the IEEE 802.11 committee proposed the use of the Wired Equivalent Privacy (WEP) protocol. WEP was proposed as an encryption protocol to provide the same level of security that wired networks had, and included 40 and 128-bit encryption at the link layer using the RC4 algorithm [85].

Unfortunately, several weaknesses and vulnerabilities were found in the protocol and that reduced the credibility of the standard for securing enterprise wide networks [23]. As a response to the weaknesses in WEP, the

Wi-Fi Alliance proposed the Wi-Fi Protected Access (WPA) as a security standard [1] for IEEE 802.11 networks. WPA introduced the use of the Temporal Key Integrity Protocol (TKIP) [80], a more hardened encryption scheme that the one used in WEP. However, the use of TKIP does not eliminate fundamental flaws in Wi-Fi security. If an attacker hacks TKIP, he or she could not only break confidentiality, but also access control and authentication [75].

Therefore, hospitals must seek security measures beyond WEP and WPA, and ensure that confidentiality and security are maintained in the network. In the following sections, an overview of some of the most common network security technologies that can be used to secure and protect wireless IEEE 802.11 networks is provided.

3.2.2 End-to-End Network Security

End-to-End network security applications include the use of Virtual Private Network (VPN) technology, Secure Socket Layers (SSL) tunnelling, IP Security (IPSec), and Kerberos network security. The application of end-to-end network security is aimed primarily at large enterprise network applications that demand higher levels of security, authentication, and confidentiality of data. The use of End-to-End network security technologies is a recommended alternative for securing enterprise wireless LANs in hospitals. In this section, an overview of the main technology alternatives is provided.

3.2.2.1 Virtual Private Network technology

Virtual Private Network (VPN) technology enables a specific group of users to access private data and resources securely over the internet or other networks [82]. VPNs use tunnelling, encryption, and authentication to provide a secure channel for exchanging data between networks. An encrypted VPN tunnel is built from the client device, e.g. a laptop or

handheld, through the wireless gateway and terminated at the VPN gateway in order to gain access to the wired LAN. All traffic passing through the wireless Access Point must go through the VPN gateway before entering the LAN. The clear text data on the other side of the secure tunnel can then continue onto its destination inside the physically secured local network. The VPN tunnel provides authentication, data confidentiality, and data integrity. Thus, other encryption mechanisms such as WEP or WPA are no longer needed.

3.2.2.2 IPSec VPNs

IPSec is a suite of protocols for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream [78]. In recent years, many protocols have been written for use with VPNs e.g. IPSec, SSL/TTS, PPTP, L2PT, and VPN-Q. These protocols attempt to close some of the security holes inherent in VPNs [47]. These protocols continue to compete with each other for acceptance in the industry and are often not compatible with each other. The use of IPSec (IP Secure) for virtual private networks has almost become the de-facto standard for securing IP data transmission over shared public data networks since VPN software has been developed for a wide variety of clients. IPSec addresses authentication, data confidentiality, integrity, and key management, in addition to tunnelling; therefore, the protocol is suitable for use in wireless networks or wired IP.

3.2.2.3 TLS/SSL Layer Security

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols which provide secure communications from clients to servers, particularly from web browsers to web servers, usually for secure connections and the exchange of sensitive data [81]. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same. TLS/SSL uses a cryptographic system that uses two keys to encrypt data - a public key known to everyone and a private or secret

key known only to the recipient of the message. TLS/SSL requires a valid site certificate issued from an recognized certificate authority. TLS/SSL provides, data encryption, mutual authentication, integrity, and non-repudiation. In a hospital setting, TLS/SSL connections will work on top of the existing network infrastructure (including wireless networks). Additionally, most web servers and web browsers today support TLS/SSL protocols and certificate based authentication and authorisation.

3.2.2.4 Kerberos Security

Kerberos is a computer network authentication protocol, which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner [79]. Kerberos provides another alternative for securing wireless networks over the air link. Kerberos is based on the key distribution model developed by Needham and Schroeder [53]. Network authentication using Kerberos involves four processes: authentication exchange, ticket-granting service exchange, user-server exchange, and secure communications between user and server. Kerberos provides both user authentication and encryption key management, and can guard networks from attacks on data in transmission, including interruption, interception, modification, and fabrication. Kerberos was voted as the "mandatory-to-implement" security service for IEEE 802.11e authentication and encryption key management. The Kerberos protocol provides features for confidentiality, authentication, integrity, access control, and availability. An interesting feature of the Kerberos protocol, is the capability for handling handoffs between Access Points and wireless clients, resulting in uninterrupted application connectivity [26]. It is mainly this feature, along with other security and authentication features, which makes Kerberos a preferred technology for securing wireless networks.

3.3 Wireless interference in hospitals

3.3.1 Interference factors

Wireless LANs in hospitals are prone to several sources of interference such as: microwave ovens, physical obstacles, cordless phones, Bluetooth interference, and other wireless LANs.

To understand the possible interference issues that may arise in hospitals, the following factors must be considered:

3.3.1.1 Physical interference and obstacles

In most medical facilities, the use of metallic surfaces, structures, and equipment has been a preferred option for many hospitals due to hygienic reasons. However, the abundance of metal in medical facilities usually presents challenges to a wireless network in terms of coverage, physical interference, multi-path propagation, and signal attenuation. Metallic obstacles such as: cabinets, drawers, stands, beds, desks, trolleys, and surgical tables may cause sporadic holes in the radio coverage of the wireless network, which in turn can influence the performance and usability of the network [36].

Although it may be impractical to remove these metallic obstacles, a simple solution to improve wireless coverage and improve signal attenuation will be to deploy additional access points or wireless LAN switches[4] in areas where there is a lack of coverage due to physical obstacles. Furthermore, the use of wireless LAN switches rather than access points prevents the problem of inter-access point interference [71].

[4] A wireless LAN switch is a device that serves as a relay station for wireless signals.

3.3.1.2 Microwave ovens

The use of microwave ovens within medical facilities and surroundings, e.g. staff rooms, cafeteria, restaurants, may present a challenge to the operation and performance of a wireless network. A microwave oven operating within close proximity to an access point will most likely cause interference and performance degradation to the WLAN if operated continuously. The reason for this interference is attributed to the operating frequencies of microwave ovens.

Microwave ovens operate at the 2.4GHz ISM (Industrial, Scientific, and Medical) band emitting wideband noise, and although shielded, they can still produce pronounced levels of radio interference or noise that can be harmful and reduce performance on wireless networks operating in the same ISM band as Bluetooth and IEEE 802.11b wireless networks. It is the effect of this wideband noise emissions that may cause interference to the WLAN. However, the performance degradation of the WLAN will only be visible during continuous operation of the microwave ovens, and depending on their use, location, and proximity with respect to wireless stations and access points, microwave oven interference to the wireless network may only be an issue for some hospitals [38].

3.3.1.3 Frequency Hopping interference (Bluetooth)

In the recent years, a wide range of Bluetooth enabled devices have been used by many hospitals worldwide. Such devices include: mobile ECG monitors, pulse oximetry sensors, cordless phones, short-range telemetry devices, bedside monitoring equipment, mobile terminals, and wireless handhelds [61].

Unfortunately, the use of Bluetooth devices continuously transmitting data presents a challenge to a wireless network since both the IEEE 802.11b and Bluetooth standards operate using the ISM band at 2.4GHz, and are incompatible with each other in terms of frequency channel allocation, which in turn causes channel interference to occur between the wireless devices.

The main problem is that Bluetooth devices do not listen before transmitting, unlike IEEE 802.11 devices which listen and if the channel is in use will defer their transmission. This poor co-existence causes interference between wireless devices and can affect the performance of a wireless network, if any Bluetooth devices are operating.

Although both standards operate within the ISM band, Bluetooth devices operate using Frequency Hopping Spread Spectrum (FHSS)[5] technology which hops over the entire 2.4 GHz band to transmit data. The IEEE 802.11b standard, on the other hand, uses Direct Sequence Spread Spectrum (DSSS)[6] technology and a given link only occupies approximately one third of the 2.4 GHz band. As a result, Bluetooth hops all over the IEEE 802.11b transmissions causing interference and performance degradation to the WLAN.

The extend to which frequency hopping interference happens depends on the utilisation and proximity of Bluetooth devices. Interference can only occur when both Bluetooth and IEEE 802.11b devices transmit at the same time at relatively close proximity. In the case of a hospital, physicians may have Bluetooth devices in their handhelds or laptops, but no interference will exist if their applications are not using the Bluetooth to transmit data.

Several Bluetooth applications, such as printing from a laptop or synchronising a handheld device to a desktop, only require Bluetooth connectivity for a very short period of time. In this case, the Bluetooth devices will generally not be active long enough to noticeably degrade the performance of an IEEE 802.11 network.

The biggest impacts are when a hospital implements a large-scale Bluetooth network, for example, one that enables mobility for physicians and nurses using handheld devices throughout the hospital. If the Bluetooth network is operational and used constantly, then the Bluetooth network will probably

[5]It takes the data signal and modulates it with a carrier signal that hops from frequency-to-frequency as a function of time over a wide band of frequencies [24].

[6]The DSSS signaling technique divides the 2.4GHz band into fourteen 22MHz channels, data is sent across one of these 22MHz channels without hopping to other channels [55].

cause a substantial number of collisions with an IEEE 802.11 network residing in the same area, thus degrading its performance.

3.3.2 Methods to reduce wireless interference

The following is a list of methods and alternatives to reducing wireless interference from and to wireless LANs in hospitals:

3.3.2.1 Ensure that wireless devices and medical equipment are compliant with EMC standards

In recent years, the Electromagnetic Community (EMC) has agreed to and adopted standards for wireless equipment operating in medical environments [41]. The initial requirements for wireless transmitting devices is that they must meet the emission and immunity requirements of the International Electrotechnical Commission (IEC) 601-1.2 or the EMC Directive 89/336/EEC in Europe [43].

Although most wireless devices might meet the emission requirements, compliance with the IEC 601-1.2 or the EMC Directive 89/336/EEC this does not mean that the wireless devices will not interfere with any medical device, only that the device's digital emissions are compliant with the industry limits and the device's digital portion has sufficient protection from interference from other electronic devices [42].

Usually, newer medical devices deployed in hospitals are designed and tested to the latest IEC/EMC standards. However, it is still possible that older devices that have not been evaluated to this standard and have been deployed thus they may cause interference problems.

3.3.2.2 Use DSSS Access Points for implementing the wireless network

The use of DSSS (Direct Sequence Spread Spectrum) Access Points for setting up a wireless network can offer several interesting advantages in interference mitigation:

- **Compliance with radio emission regulations**

  Most of the access point products in the market today are designed to be compliant to stringent "Class B – Spurious Emission" requirements outlined by the IEC and the EEC, which may prevent access points from interfering with medical devices.

- **Transmit power configuration**

  Most industrial DSSS access points have a feature for configuring the radio transmission power of the access points. Radio power management allows DSSS systems to be configured to operate at lower power levels, which reduces the likelihood of interference to installed medical equipment. Power output levels can be reduced to as low as 1mW if required to reduce radio cell sizes and coverage reach.

3.3.2.3 Limit the use of Bluetooth enabled devices

Since it may not be practical to completely forbid the use of Bluetooth devices in the hospital, it is important that the use of such devices is limited in order to avoid potential interference problems with WLANs in medical facilities. As a good recommendation, wireless Bluetooth devices must not be used in close proximity to IEEE 802.11b stations or access points in areas where there is high dependency upon the WLAN, e.g. in intensive care and cardiology units, etc. An additional measure would be to limit and manage the use of Bluetooth devices by establishing a regulatory group within the hospital for managing unlicensed wireless devices. Guidelines and policies for using wireless devices should be established by this group to avoid interference issues in medical facilities.

Chapter 4

The Patient Identification Prototype

This chapter describes the design decisions made for the construction of the patient identification prototype. Several technical choices were evaluated in terms of the software and hardware used in the prototype. A description of how the prototype was constructed is also given in this chapter.

4.1 Prototype features and requirements

The initial features and requirements for the prototype were to provide a simple, but yet useful system that can be used by the medical staff to identify patients. Due to the mobile nature of the medical staff, it meant that the system had to be based on a portable handheld device, e.g. a PDA. Taking this as a requirement for the prototype design, the next question was what hardware and software features were required for making wireless patient identification possible. The following, is a summary of the most relevant features and requirements that were considered for the design of the RFID patient identification system prototype.

4.1.1 Web-based Interface

This feature is a requirement in order to simplify the access to medical information via the device. Information about the patient coming from the HIS (Hospital Information System) must be accessed through a web-interface. This is to simplify interoperability between handheld devices and avoid the need for designing a specific platform dependent application.

4.1.2 Software application independent

The prototype should implement a feature that will allow the reading of tag information and access the RFID reader interface using any application that runs on the handheld device, e.g. work processor, web browser, spread sheet program, etc. The requirement for implementing this feature is to be able to access and re-use tag information using any program, and to avoid the need to develop modified versions of each such application. Therefore, the software interface for accessing the RFID reader on the prototype should be application independent. For this requirement, we evaluated several techniques and software approaches, which are discussed in section 4.2.2.

4.1.3 No storage of patient data on the prototype

This requirement is important to prevent any possible privacy problems in cases when the patient identification prototype is damaged, stolen, lost, or violated.

4.1.4 Longer reading range

This feature is important to facilitate reading tag information from a longer distance. Currently, most commercial RFID readers on the market only provide short range reading of RFID tags (5 to 10 cm approximately). For some applications such as healthcare, it is desirable that the RFID readers have a greater reading range. However, the implementation of this feature ultimately depends on the design of the RFID antenna (see section 4.2.1).

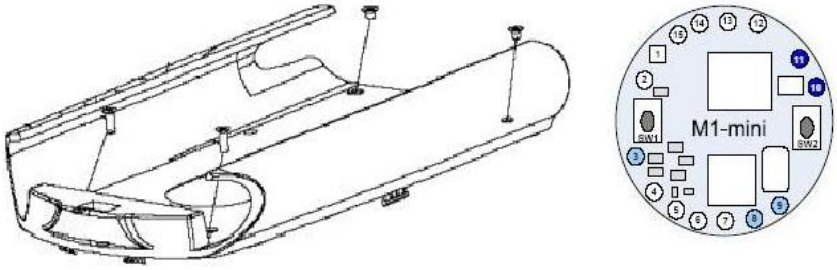

Figure 4.1: iPAQ expansion pack and Skyetek M1 reader diagrams.

4.2 Evaluation of design choices

In this section, an overview of some of the design choices that were used to construct the prototype are presented.

4.2.1 Hardware choices

4.2.1.1 Handheld device

The handheld device that was chosen for the implementation and development of the RFID prototype was the Hewlett-Packard[1] iPAQ h5555. The iPAQ h5555 is one of the most popular handheld models in the market today [77]. The particular model we used for constructing the prototype had features for extending its hardware interface (derived from the Compaq iPAQ H3600 series), thus, allowing users to plug-in experimental hardware modules, these features made the iPAQ h5555 a good choice to implement and develop the patient identification prototype.

[1]Also know as the PocketPC, note that this term is also branded by Microsoft to refer to handhelds that run the Windows CE or Windows Mobile operating systems.

4.2.1.2 iPAQ Expansion Pack Interface

For constructing the attached RFID hardware module, we used the iPAQ expansion pack interface. An iPAQ expansion pack has features for interfacing to the iPAQ h5555 via a 100-pin connector, which can be used as a serial, parallel, and SPI bus, as shown in figure 4.1.

For the development of the prototype, we use the serial RS-232 interface on the iPAQ expansion pack interface, since the Skyetek M1 reader (see below) can be interfaced through the RS-232 port.

4.2.1.3 RFID Reader Hardware Module

The RFID reader hardware module chosen for the construction of the prototype was the Skyetek M1 RFID reader module, as shown in figure 4.1. The Skyetek M1 RFID reader is a multi-protocol RFID reader, low power, with a RS-232 serial interface and a SPI bus interface [15]. The reader is small enough that it can be attached to the iPAQ expansion pack PCB or wired directly to the iPAQ expansion pack connector ports, which provide power, data, and communication. In our approach, it was decided that the Skyetek M1 RFID reader would be attached to the iPAQ expansion pack connector via a wired RS-232 serial interface and powered via the iPAQ expansion pack connector.

4.2.1.4 Antenna design choices

During the development of the RFID patient identification prototype, we considered several antenna designs for the RFID reader. Below, we overview some of the preferred options for designing the RFID antenna.

- **Build-in reader antenna**

  This is the approach that many commercial products take. Available RFID readers on the market, e.g. such as the Skyetek M1 RFID reader,

usually come with an internal or build-in antenna[2], usually embedded on the printed circuit board. The benefits of this approach are that no additional circuitry, i.e. external antenna, is needed to operate the RFID reader, at the same time hardware costs are minimized because there is no need to purchase components and materials for the extra circuitry. However, the disadvantage of this approach is the limited reading range of the RFID reader due to the internal antenna size limitations.

- **External loop antenna**

  Loop antennas are used predominantly in supply chain RFID applications (where thousands of tags need to be read rapidly and several times), they can provide the necessary range/coverage, and be mounted in warehouses as part of the production line or supply chain.

  The reading range of the loop antenna is proportional to the size of the inductive loop on the antenna, this implies that a large loop antenna would need to operate at higher currents, therefore, requiring more power to operate. A flexible feature of loop antennas is that they can be designed and customised to the desired range and power by adjusting the inductive loop of the antenna.

  An external loop antenna can be connected to extend the reading range of the handheld RFID reader. Unfortunately, this approach has several disadvantages, namely, the size required by the loop antenna (depending on the required reading range, a loop antenna may prove to be bulky in some cases) and the power to feed the antenna would also be a limitation in terms of power consumption.

  In practical terms, a RFID loop antenna can be easily designed and built (with copper wire or embedded as part of the PCB), and its components easily acquired, however, the reading characteristics of loop antennas vary if they are not properly tuned, and the development time

[2]This build-in antenna, is actually a small loop antenna, that is part of the RFID reader module.

would depend on the availability of materials and prototyping facilities.

- **External Fractal antenna**

  As part of the literature review for the RFID antenna design, we overviewed the use of fractal antennas. Fractal antennas have been around and under development in the recent years, with applications ranging from short and long range telecommunications, advanced military, and supply chain applications.

  Notable features of fractal antennas is that they can be capable of operating optimally at many different frequencies simultaneously (making them suitable for the design for wideband applications). In addition, they can be easily manufactured and printed on most surfaces (in the case of a printed circuit board the antennas can be scaled and printed in any size). Many fractal antennas use the fractal structure as a virtual combination of capacitors and inductors. This makes an antenna that has many different resonances, that can be chosen and adjusted, by choosing the proper fractal design (it also shrinks the antenna compared to conventional designs, and does not need additional components). Therefore, the complexity of designing fractal antennas resides in matching the fractal pattern and the desired resonant frequencies. This complexity is usually addressed at design time with the help of antenna design tools and simulators.

  Although it is practical to design a simple fractal antenna based on existing fractal models, e.g. Sierpinski-gasket, Koch-snowflake, and Hilbert curves. Most suitable fractal antennas designs today are already protected by patents[3], and due to the licensing of patents and possible costs associated, a more comprehensive literature review and patent search should be conducted to avoid infringing existing intellectual property.

  Thus, for several of the reasons mentioned above, designing a fractal antenna was not a feasible option for the prototype.

[3]http://www.google.com/patents?q=Fractal+antennas&btnG=Search+Patents

- **External Meander Line antenna**

  Another type of antenna design that was evaluated was the use of high directivity meander line antennas. Meander line antennas have become quite popular in the recent years, due to their compact/small size, and their high directivity properties. Meander line antennas are an attractive option for use in RFID readers since they can fit into smaller hardware modules and can operate in multi-mode (it can have multiple radiation modes), which could be useful for adapting the reader to the different RFID protocols and reading ranges. Unfortunately, the cost of a meander line antenna prototyping kit was not within the budget of the project, and evaluation and experimenting with meander line antennas was not possible.

After the literature review and evaluation of several antenna designs, we had to select a design that would accommodate both the time-frame of the project and the project's budget. The decision regarding the antenna designs was influenced by the complexity, cost, and required time to build a working antenna.

The first two designs considered, the build-in and external loop antennas, seemed a feasible option to build an initial system quickly and at the lowest cost. The complexity requirement for the build-in antenna was minimal, since most RFID reader modules come with such an antenna. The complexity for the external loop antenna, implied that a loop antenna had to be designed either external to the RFID module or as part of the PCB design. Furthermore, the external loop antenna would have to be tuned to the desired reading range characteristics of the RFID reader. The time requirement for developing an external loop antenna could be short in some cases, as it mostly depends on the time to receive the needed materials, or to manufacture a test PCB.

The designs for the fractal and meander line antennas, although greatly desired for building the prototype, proved to be too expensive, and the development and testing time would be long (due to the learning curve required for working with these antenna technologies). The design for a

fractal antenna was evaluated initially, since fractal antennas can be build using materials similar to external loop antennas, however, due to the lack of available design tools and design experience, using a fractal antenna was not considered a suitable choice.

Due to development time considerations (keeping the development time constrained to five months) and availability of materials for experimenting with other antenna designs, the build-in antenna was selected as the most feasible and available option to use in the patient identification prototype.

4.2.2 Software choices

4.2.2.1 Operating System Choice

The operating system used for developing the software for the RFID prototype was Microsoft's Windows Mobile 2003 OS, which runs on most iPAQ and PocketPC hardware and it is supported by a wide range of development tools and third-party software libraries [84]. One important feature of the Windows Mobile 2003 OS is that legacy Win32 APIs can be used (similarly to existing Microsoft operating systems such as Win 95/98/ME and Windows NT) a feature that aids a developer familiarize with these API functions [83]. Therefore, programming hardware, e.g. serial, parallel, and network interfaces, through the Win32 APIs can be done virtually in the same way as in other Microsoft operating systems, allowing re-use of existing APIs, and helped reduce development time.

4.2.2.2 Software Interface for the RFID Reader

The preferred option for developing the RFID software interface was to develop a program that could be interfaced with over a web interface using the PocketPC's web browser. The choice for using a web interface as opposed to a fixed program, was done primarily to prevent storing of patient data and to avoid possible privacy issues if the prototype is damaged, stolen, or

violated. Using a program that can interact via the web interface, we simply relay the required patient data, e.g. when the patient RFID tag is read and the patient is identified via an ID number.

Therefore, the aim was to design a program that would allow access to the RS-232 interface of the h5555 PocketPC which in turn would access data from the attached Skyetek M1 RFID reader, and relay this data to the web browser. This program, would have to serve as the main interface to the M1 RFID reader and would have to run on the PocketPC.

Information such as patient ID, physician ID, etc. can be relayed via the program (assuming that this information would be read from the RFID reader's serial port via the iPAQ expansion pack connector on the h5555) to the web interface using the fields of the web page, as shown in figure 4.2.

For this reason, we considered several technologies and software design alternatives, these are covered in more detail below:

ActiveX Controls

The use of ActiveX controls was considered at first to interface the RFID reader with the Care2x hospital information system, because of the simplicity and accessibility of ActiveX controls to interface with the host operating system. However, we found some limitations in our approach; primarily, the functionality of ActiveX controls to access hardware resources and security. The most notable, was the limitation of the PocketPC's browser to fully run our serial ActiveX controls (a control to access and read data from the h5555's serial port). The current version of the PIE (Pocket Internet Explorer) v4.0 included on the Windows Mobile 2003 OS (aka Windows CE 4.0) claimed to provide full support for ActiveX controls, however, in practice, we could not run and access the serial port hardware through our serial ActiveX control.

Secure Java Applets

The use of secure java applets was considered because of the benefits of platform independence and browser integration. The typical features

of java applets are that they can run over a web interface using java supported browsers. Unfortunately, the approach to use java applets to develop the RFID software interface had a similar disadvantage to the ActiveX approach; currently, the available version of the Pocket Internet Explorer has limited support for all the necessary features of java applets. Also, at the time of this writing, this same limitation applied to other internet browsers that run on the PocketPC.

Software Wedge

A software wedge is a program interface that captures input data (usually from a hardware acquisition device or sensor) and feeds this data to the application where you want the data to go. Using a software wedge interface the user gains more control over how and where the input data is used. A software wedge can be seen as a middleware interface which acts between a data capturing device (such a barcode reader or a RFID reader) and the user program. A software wedge is independent of any program and it is usually installed and used as a special function which works as part of the operating system, i.e. similar to a special driver or plug-in device. Software wedges can be easily developed (using any programming language that can access hardware resources such as C, C++, .NET, and Java) and customised to work over most communication ports, e.g. serial port, parallel, keyboard, etc.

After developing several prototype programs using the approaches described above, we decided that the most flexible and feasible approach to access and interface the Skyetek M1 RFID reader would be to use a software wedge.

Figure 4.2: Single button UI software wedge using the SIP interface.

4.3 Prototype construction and development

4.3.1 Software Design

4.3.1.1 Software wedge for the RFID reader

As stated earlier, we selected the software wedge approach to develop the software interface for the Skyetek M1 RFID reader module. In order to create a 'wedge' interface that could access the M1 reader, we programmed our software wedge interface in C++ using the Soft Input Panel API included as part of the Microsoft Windows Mobile 2003 operating system [57]. For this, we needed to define what our user interface for the accessing the RFID reader would look like. For prototyping purposes, we decided to use a 'single-button' user interface (as shown in figure 4.2).

Since the SIP control would need to interface to the local serial port (which is directly connected to the Skyetek M1 reader's serial port) on the PocketPC, we used the Win32 legacy APIs to configure the serial port (see code listing 4.1). The initial parameters used to program the Skyetek M1 reader module are show in table 4.1.

Parameter	*Value*
Baud	9,600 Kbps
No. of bits	8
Stop bit	1
Parity	None

Table 4.1: Skyetek M1 RFID serial port settings

Listing 4.1: Configuring the serial port on the PocketPC.

```
1  int ConfigurePort(int BaudRate,int ByteSize,int Parity,int StopBits)
2  {
3    CommSettings.BaudRate = BaudRate;
4    CommSettings.ByteSize = ByteSize;
5    CommSettings.Parity   = Parity ;
6    CommSettings.StopBits = StopBits;
7
8    /* Line Feed (LF) character */
9    CommSettings.EvtChar = 0x0D;
10
11   isPortReady = SetCommState(CommPort, &CommSettings);
12
13   if(isPortReady == 0)
14   {
15     CloseHandle(CommPort);
16     return FALSE;
17   }
18   return TRUE;
19 }
```

4.3.1.2 RFID Reader Communication Protocol

In order to be able to read and write to the RFID tags/wristbands we had to communicate with the Skyetek M1 reader through a protocol. The Skyetek M1 reader came with a pre-programmed protocol and commands that can

Parameter	*Bytes*$(n+1)$	*Example*
PID Nr.	8	16359854
Registration date	10	19/03/2005
Registration time	5	16:46
Title	3	Ms
Family name	20	Bennet
Given name	20	Angela
Date of birth	10	03/08/1965
Blood group	2	B
Civil status	12	Married
Address street	20	42 Cluan Dara
Town/City	20	Galway
Country	20	Rep. of Ireland
Insurance Nr.	15	16958456
Insurance company	20	VHI
Telephone	20	+35391559403
PPS	15	4657897A

Table 4.2: Data format of the RFID wristband.

be used to access the reader, using an API [16]. We used this API to be able to read and write to the RFID tags/wristbands.

4.3.1.3 Reading the patient wristband

For initial testing purposes, the software wedge only read the patient ID from the tag and put it onto the form field where the user wanted to place this information. Figure 4.3 shows the steps required for reading data from the patient RFID wristband.

If specific information from the tag was needed, e.g. the insurance number, blood group, civil status, etc, then an additional pull-down menu was planned to be added as part of the software wedge interface to allow the user (once the tag was read) to select the specific data he/she wanted from the tag. However, during the development of the pull-down menu, it was not possible to program a functioning pull-down menu that could work using the SIP interface.

If the user needed to read all the patient data stored in the tag/wristband, another approach would have been, to add an additional button to the software wedge that would read all the patient data from the tag (in one single read) and be able to place it, for instance, onto a pre-defined electronic form in one single click. In this approach, the software wedge would act in the same way as a keyboard interface, e.g. allowing the user to select one field on the form and input text and move between the fields on the form as if the user is "typing" such information; in this way, the software wedge could have been programmed to fill-in all the text fields in a form.

Alternatively, a much simpler approach, would have been to store the patient data into the tag/wristband using XML, and then once this information is read, the information can be easily forwarded to a web server (if using a web interface to input the data) so that it can be easily processed at the server side.

For initial prototyping purposes, the format used to store patient information in the tag/wristband was based on a very simple text format[4] which consisted in allocating data according to the required size for each of the data fields as shown in table 4.2. For each data field stored in the tag, a number of bytes was allocated to find the off-set of each data field and easily read the data. The delimiter of each data field was the length in bytes assigned to the fields, also shown in table 4.2.

The patient identification prototype was programmed to only read information from the RFID wristbands, assuming the RFID patient wristbands would be programmed before they were used with the prototype, i.e. by

[4]By text format, we mean, storing data using ASCII standard characters.

hospital staff at the admissions clinic.

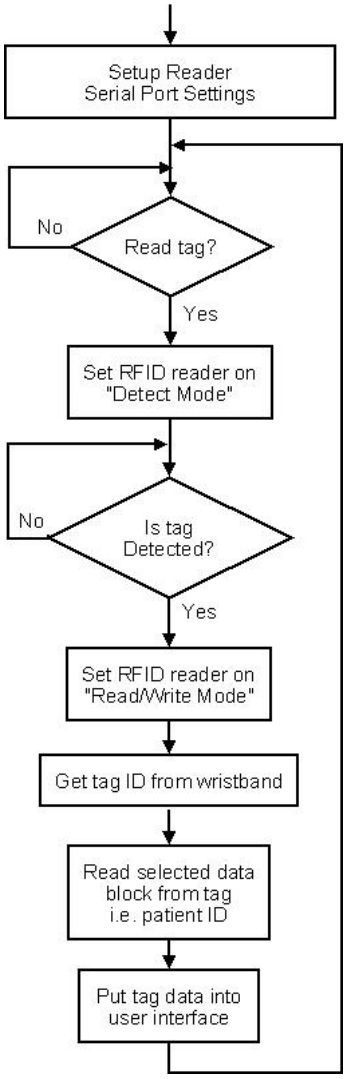

Figure 4.3: Flow-chart for reading data from the patient wristband.

4.3.1.4 Programming the patient wristbands

A special java program was developed to program the RFID patient wristbands with patient information, e.g. patient names and ID number, this information was then be used to test the functionality of the patient identification prototype (see section 5.3).

Listing 4.2 shows a section of the java code used to program the RFID wristbands with factious patient data.

Listing 4.2: Programming the Patient ID onto RFID wristband.

```
1  public void WritePatientID()
2  {
3    String TagID = "E007000001F9B313";
4    String PatientID = "12345678";
5    String WritePatientID = "\r" + "0844010003" + PatientID + "\r";
6    String SelectedState = \n" + "481401" + TagID + \n";
7
8    try
9    {
10     /* Set RFID reader to read/write mode */
11     serialDataOut.write(SelectedState.getBytes());
12     System.out.println(SelectedState);
13
14     Thread.sleep(2000); /* wait 2 seconds */
15
16     /* Write the patient ID onto the tag */
17     serialDataOut.write(WritePatientID.getBytes());
18     System.out.println(WritePatientID);
19
20   } catch (IOException e)
21   {
22     e.printStackTrace();
23   }
24 }
```

4.3.2 Hardware Construction

Figure 4.4 illustrates the main components involved in the construction of the prototype. The prototype consists of the following components:

- **iPAQ connector port:** The iPAQ connector port connects the h5555 PocketPC and the Skyetek M1 reader together.
- **PCB mount:** The PCB is used to mount the Skyetek M1 reader and the iPAQ connector port components.

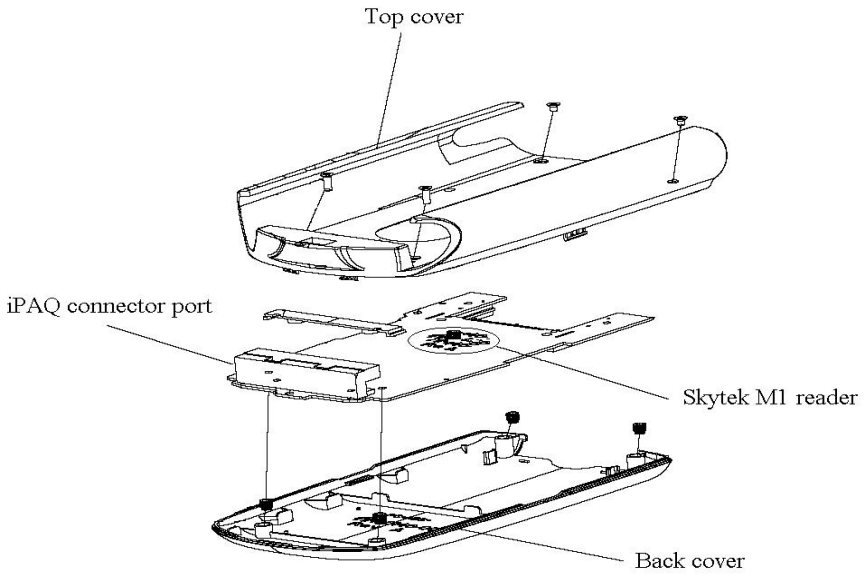

Figure 4.4: Patient identification prototype component diagram.

- **Skyetek M1 reader:** The skytek reader is attached to the PCB component and wired to the iPAQ connector port. Figure 4.5 shows the wiring diagram used for connecting the Skyetek M1 reader to the iPAQ connector port.
- **Top/Back covers:** The top and back covers form the casing of the iPAQ expansion pack. The covers are joint together to protect and seal the internal circuitry, e.g. the Skyetek M1 reader and other PCB components.

Figure 4.6 shows the actual assembled version of the patient identification prototype, and figure 4.7 shows the actual components used in the construction of the prototype. In the next chapter, a description of how the prototype was used for identifying patients is given.

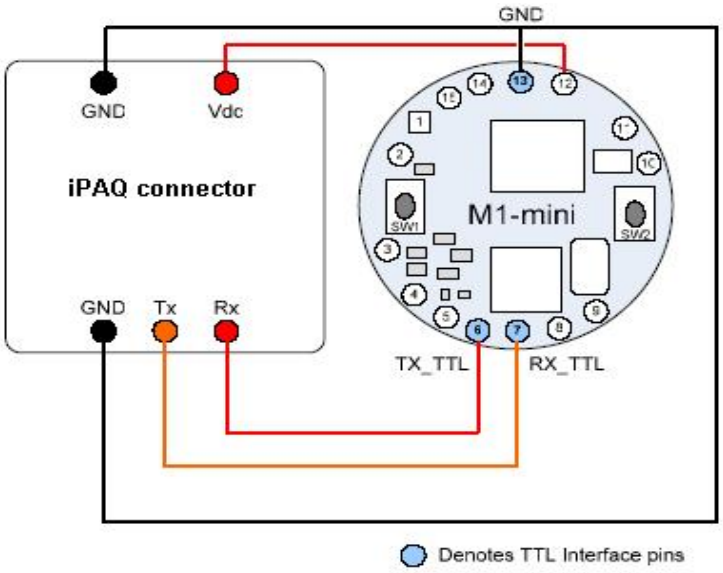

Figure 4.5: Wiring diagram for the Skyetek M1 reader and iPAQ connector.

Figure 4.6: Actual version of the patient identification prototype.

Figure 4.7: Patient identification prototype components.

Chapter 5

Testing the Patient Identification Prototype

This chapter describes how the patient identification prototype was tested. It describes how the software interface for the prototype was used to identify users/patients. This chapter also comments on the effects and benefits that the prototype could have in the care of patients.

5.1 Infrastructure and test-bed configuration

To test and evaluate the functionality of the prototype, we created a test-bed which consisted of a wired and wireless network, the Care2x Hospital Information System, the patient identification prototype, and several RFID wristbands (as shown in figure 5.1).

The following is a detailed description of the components used:

- **Patient Identification Prototype**

  The patient identification prototype has already been described in the previous chapter.

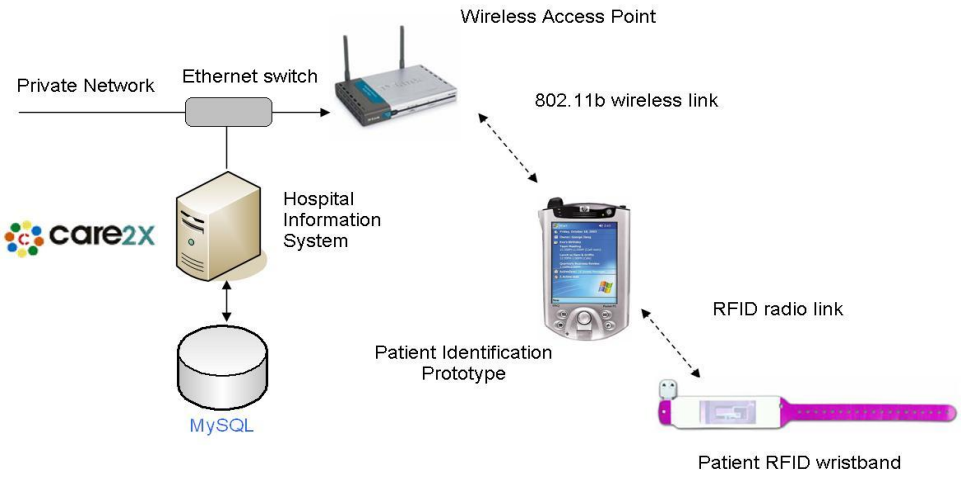

Figure 5.1: Test-bed infrastructure.

- **RFID Wristband**

  The RFID wristbands used to test and evaluate the functionality of the patient identification prototype were based on the Tag-it HF passive RFID chip (operating at 13.6MHz) from Texas Instruments [31]. The wristbands used were pre-programmed with fictitious patient information (see section 5.4).

- **Wireless Access Point**

  To provide wireless connectivity, a Cisco Aironet 1200 access point (AP) was used [70], the AP was configured to operate using the IEEE 802.11b wireless standard and was connected to an Ethernet switch. The access point was configured to provide IP addresses to the associated wireless clients.

- **Care2x Hospital Information System**

  We used Care2x [39] as the hospital information system. Care2x is a web based Hospital Information System that consists of several modules, e.g. laboratory, radiology, nursing, etc. that can be integrated with the other medical information systems or used as a stand-alone centralized system.

The Care2x hospital information system was set-up in a Linux desktop (2.6GHz Pentium 4 processor, 40GB hard disk, 256MB memory). Care2x was connected directly to the wired local network via an Ethernet switch.

5.2 Use case

In order to test the functionality of the patient identification prototype, we formulated a use case (as shown in figure 5.2).

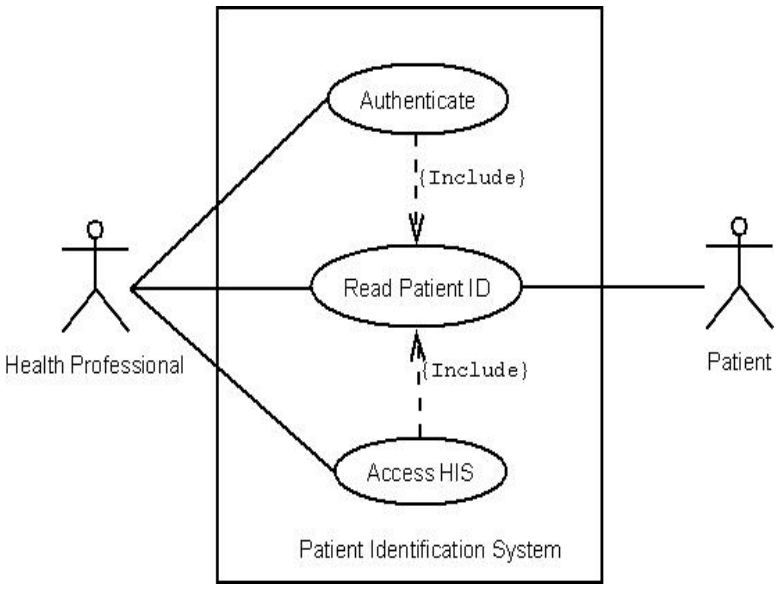

Figure 5.2: Use case diagram.

For our use case, we decided to used the patient identification prototype to read the patient ID number from the patient's wristband, then display the patient's demographic and hospital admission details.

5.2.1 Actors

- **Health Professional**: A health professional who needs to identify and requires access to the medical information about a patient, e. g. a medical practitioner, pharmacist, nurse, or midwife.
- **Patient Identification Prototype**: An electronic system which provides the means to identify a patient and provide information about the patient for a particular area of care.
- **Patient**: Person for whom medical services are to be provided.

5.2.2 Activity diagram

The diagram shown in figure 5.3 describes the interaction of activities for identifying a patient using the patient identification prototype.

5.2.3 Process flow

Below we describe the process flow for our use case:

- We begin by authenticating the health professional who is to use the patient identification prototype, e.g. by using a PIN (Personal Identification Number) or a password, to allow the health professional to use the patient identification prototype.
- The health professional accesses the HIS using the web browser in the patient identification prototype, e.g. using Pocket Internet Explorer. The health professional accesses the HIS interface and searches for a patient (using the search field in the Care2x web page).
- The health professional selects the software wedge interface on the patient identification prototype to put the RFID reader in "Detect Mode". This allows the health professional to use the patient

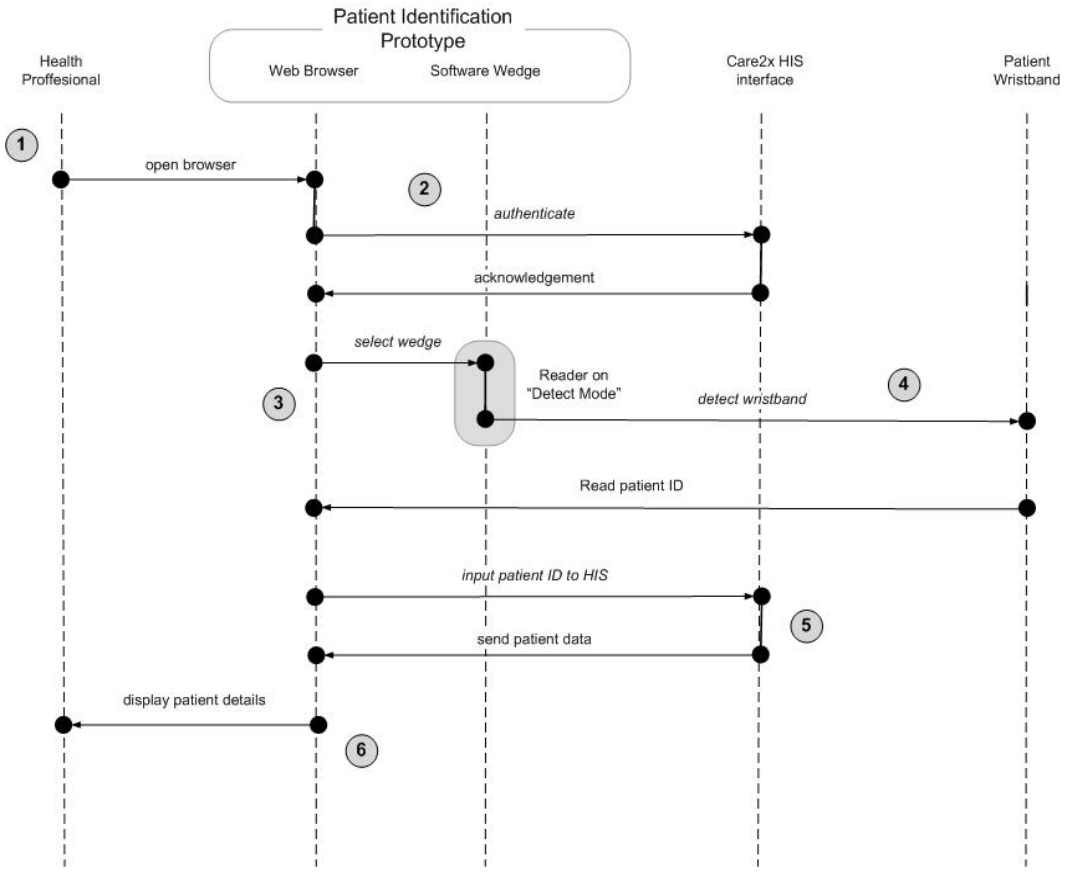

Figure 5.3: Activity diagram.

identification prototype to detect and read the patient's wristband when in close proximity to the prototype.

- Once the patient wristband is detected. The patient identification prototype will read the patient ID from it.
- The patient ID is then input into the search field in the HIS interface (using the software wedge). The HIS interface then displays the patient demographic and hospital admission details using the web browser of the patient identification prototype (as shown in figure 5.8).

5.3 Using the prototype to identify a patient

To identify a patient using the prototype, the user has to follow the steps illustrated in the following figures.

Figure 5.4: Search a patient in Care2x.

- Open the Care2x interface using the Pocket Internet Explorer and enter the Care2x login details to access the system. Once logged-in to Care2x, the user selects to 'search for a patient' (as shown in figure 5.4).
- Select the RFID software wedge interface as the input method, as shown in figure 5.5.
- Put the RFID reader into "Detect Mode" by pressing the "Scan" button (as shown in figure 5.6). This will enable the RFID reader to detect any patient wristbands in proximity to the RFID reader on the prototype.
- Once the patient identification prototype is in detect mode, the health

Figure 5.5: Selecting the software wedge for the RFID reader.

professional brings the back of the prototype in close proximity to the patient's RFID wristband to read the patient ID number from this wristband, as shown in figure 5.7.

- After the patient's ID is read from the wristband, an 8-digit number will appear in the "search patient field" of the Care2x web page (as shown in figure 5.8), and the page will automatically re-direct to another page which displays the demographic and admission details about this patient (as shown in figure 5.9). From that page, the user can retrieve other patient information (e.g. laboratory results, nursing reports, pre-inscriptions, etc.) via Care2x.

Figure 5.6: Detecting the patient's RFID wristband.

5.4 Evaluation of the prototype

To evaluate the functionality of the prototype, we used the following criterion:

1. What effect does the prototype have for patient identification.
2. What effect does the prototype have for retrieving information about patients.
3. What effect does the prototype have for accessing and viewing information about patients.

Initially, we wanted to evaluate the performance and functionality of the patient identification prototype against current practices (patient identification and access to patient information) in the hospital using real patient data, and in a real scenario.

Figure 5.7: Reading the patient ID from the patient's wristband.

However, in order to use the prototype, we would need to obtain permission and consent from the patients in order to store their demographic details in the RFID wristbands, and link that information to Care2x.

Due to privacy concerns and data protection regulations, we could not obtain permission from the hospital to use real patient data or access any patient related information or medical records (additionally, it was very difficult to obtain consent from individual patients). Similarly, we could not obtain permission from the hospital IT staff to interface Care2x with the existing hospital information systems at the hospital.

To overcome this, we created a small data-set which contained fabricated medical information concerning fictitious patients (including fictitious demographic details and hospital admission details). The data-set consisted of 40 patients with even distributions of male and female patients. We installed this data-set in a local version of Care2x (running as part of our test-bed infrastructure). Then, we randomly programmed several RFID patient wristbands with some of the fictitious patient information from the data-set (for simplicity, we only programmed the patient ID number in the tag). Then,

Figure 5.8: Patient ID number read from the wristband.

we used the prototype to identify and read each of the wristbands individually (and followed the steps described in section 5.3), and made observations on the effects that the prototype could have for improving patient care.

5.4.1 Observations and effects on patient care

It was difficult to fully evaluate the prototype against the chosen criterion, since the hospital (University College Hospital Galway) had very few departments fully computerised (which was an important requirement to operate our prototype and integrate Care2x to access patient information), with most departments using paper-based medical records and processes, as the means to access information about patients. Therefore, the evaluation of the prototype was mainly done via observations and manual comparisons

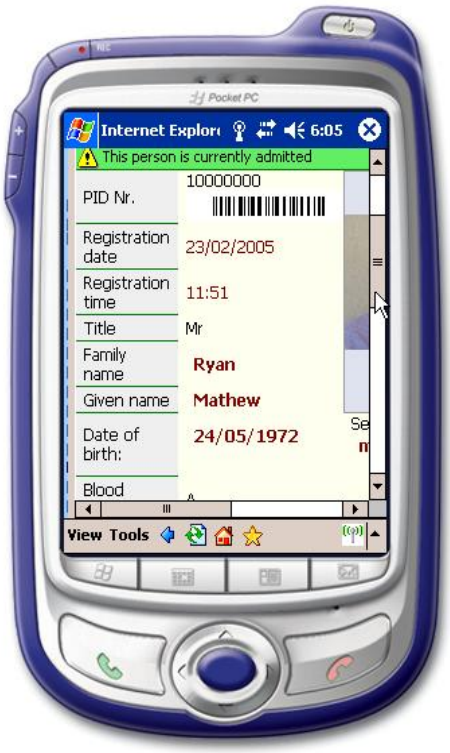

Figure 5.9: Patient demographics and admission details.

with current practices in the hospital.

The following, are the most notable observations we made during our evaluation:

5.4.1.1 Prevention of patient misidentification

The prototype introduced the use of a 'tool' in the patient identification process (the existing practice for identifying a patient in the hospital relies upon visual and chart-based identification methods). This means, that if the medical staff wanted to take short-cuts to identify a patient, the use of the prototype would quickly discourage this. An example of this, is that the medical staff would need to identify themselves first (by reading their RFID batch/card, etc.), before they could identify the patient. In

this way, if medical services are performed for the patient, an audit trail would exist, and allow the tracking of interactions (including medications and prescriptions) of the patient, which in turn would help to reinforce patient safety procedures. Since the prototype may prevent the medical staff from deviating from the required identification procedures, this effect could contribute to the prevention of patient misidentification.

5.4.1.2 Improved retrieval of patient information

The use of the prototype allowed the user to have improved access and retrieval of patient information. Since the prototype is a wireless portable handheld device, this allowed the users, e.g. doctors, nurses, etc. to retrieve patient summaries, admission details, medical reports, and other sections of the patient record, more easily via the Care2x web interface.

This means, that the medical staff could retrieve patient information (assuming the user who requests this information has the proper access and authorisation rights) at the point-of-care or remotely more easily.

The improved retrieval and access to patient information is possible because patient information is stored electronically, and can be displayed via a web browser interface. This improvement is especially visible in hospitals that are not fully computerised, and in hospitals that still rely in paper-records to access patient information.

5.4.1.3 Accurate patient information on display

We also observed that, in addition to improved access to patient information, there was an improvement in the accuracy (in terms of legibility and readability) in the patient information on display, e.g. in the screen display of the handheld.

In hospitals that use paper-based records, it is common to have the patient's entire medical history on a paper folder or chart, where sheets of paper are compiled and attached as needed, e.g. laboratory results, notes, reports,

etc. One of the main problems with such paper records, is that medical information contained in them may have been poorly written, or with illegible handwriting. Because the patient information was displayed in electronic form in the prototype, this facilitated the reading of patient information and prevented the misinterpretation of medical information.

Chapter 6

Conclusions

Since the scope of this thesis covered a very wide problem area, we list and summarise the most relevant conclusions obtained from the project.

Patient misidentification will remain an important problem to be acknowledged and managed by many hospitals. Without suitable patient identification systems in place (electronic systems or guideline based systems), the risk to patient safety and medical malpractice will remain on the increase.

Similar to barcode applications in healthcare, RFID has found intriguing applications for improving the accurate delivery of care to patients. From one perspective, RFID patient identification systems would seem to provide a greater return-on-investment than barcode, due to the adaptability of the technology in hospitals. However, RFID positive patient identification systems will only be able to be deployed in hospitals that have an acceptable level of sophistication (including integration and interoperability) in terms of their IT and hospital systems to take advantage and derive benefits from the technology. Today, most hospitals are reluctant to abandon their initial investments in barcode identification systems simply to introduce new technology replacements. Hospitals that do not have electronic patient identification systems in place, may also be reluctant to use RFID patient identification systems due to the still high cost associated with RFID

compared to existing barcode systems. Most likely, in the future, barcode and RFID systems would need to complement each other in terms of functionality, cost, and usability. But until that happens, the preference of barcode identification systems over RFID systems will remain unchanged.

The use of wireless networks, combined with the use of clinical information systems, adequate training of medical personnel, IT and network support, and the use of wireless handheld devices could provide the ability to improve the quality and delivery of healthcare in hospitals. Using wireless LANs in a medical environment can greatly improve the productivity of care providers and the accuracy of diagnoses and treatment by facilitating the retrieval of patient related clinical information by physicians. However, several open issues such as security, data privacy, wireless interference, and wireless network maintenance must be addressed accordingly in order to successfully deploy and use the technology in hospitals. Similarly, another important issue that remains prevalent, is the limited operational time of handheld devices. To date, this is the *most significant weakness of handheld devices*. To be used continuously in a hospital setting, the medical staff requires average continuous operational times of up to 20 hours to be able to use these devices. To some extent, this issue, would limit the use of any handheld based identification system.

The concept of a wireless patient identification system was demonstrated and evaluated in this project. With the patient identification prototype we demonstrated and observed that by introducing a "patient identification tool" into the care process, there could be improvements in patient identification procedures (with possible benefits to patient safety), easy retrieval and access to patient information, and that those improvements can facilitate the delivery of medical services to patients in hospitals.

6.1 Future Work

In retrospective, we identified several technical decisions made during the development and construction of the prototype which could have impacted

the future development of the patient identification prototype. As we worked in the project, we discovered that the iPAQ expansion pack interface was discontinued by Hewlett-Packard (although discontinued officially by Hewlett-Packard in 2004, previous h3000 and h5500 PocketPC series models and legacy accessories still remain available from different vendors) and future models of the PocketPC (hx2400 series) would not support it[1].

As future work, alternative hardware approaches to re-design the patient identification prototype would consider the RFID reader hardware to be attached to a SDIO (Secure Digital Input Output) card, or that the RFID reader could be designed as a hardware module as part of the SDIO chip.

In addition, a similar approach would be to design a SDIO card with barcode and RFID functionality as part of a system-on-chip. Due to space limitations in the SDIO card, a suitable RFID antenna solution would be to use meander line antennas.

Alternatively, a 'commercial' approach would be to involve the OEM (Original Equipment Manufactures) handheld vendors to include RFID functionality in their products, with the expectation that this may aid many industries (such as healthcare) in using RFID in future technology applications, and facilitate the adoption of RFID as a mainstream wireless technology.

[1]Similarly, the Compact Flash card interface was not included in newer models.

Bibliography

[1] Wi-Fi Alliance. Overview of Wi-Fi Protected Access WPA. *Wi-Fi Alliance, http://www.wi-fi.com*, October 2002.

[2] S. Anderson and W. Wittwer. Using bar-code point-of-care technology for patient safety. *Healthc Qual, Nov-Dec; 26(6):5-11*, 2004.

[3] K. Arabe. The State of RFID: Move Over Bar Codes. *Industrial Market Trends*, October 2002.

[4] F. Baldwin. Believing in Biometrics: Biometric technologies not only exist – they work and are now affordable. *Healthcare Informatics*, August 2000.

[5] R. Blair. Like it, Yes. Need it, Yes. Buy it, Nah. *Health Management Technology Journal*, September 2005.

[6] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. *CiteSeer.IST Scientific Literature Digital Library*, 2001.

[7] J. Brown. Trust installs wireless at eight London hospitals: 7,000-user network supports UCLH project to replace paper processes. *Computing Magazine, UK*, September 2005.

[8] T. Castle. Online Authentication using Combined SmartCard and Fingerprint Recognition. *Centre for Applied Research into Education Technology, University of Cambridge*, August 2001.

[9] D. Chadwick. Smart Cards aren't always the smart choice. *IEEE Computer Magazine*, December 1999.

[10] L. Chroust. Deploying Wireless LANs : Today's smart planning helps wireless users to add and expand well beyond tomorrow. *Health Management Technology*, August 2001.

[11] K. Chung. Elimination of medication errors through positive patient medication matching. *Avante International Technology, Inc.*, December 2001.

[12] J. Collins. Hospitals Get Healthy Dose of RFID. *RFID Journal Inc*, April 2004.

[13] European Commission. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Office of the Data Protection Commissioner. 3rd Floor, Block 6, Irish Life Centre, Lower Abbey Street, Dublin 1, Ireland.*

[14] HBS Consulting. SmartCards in healthcare. *HBS Consulting*, January 2004.

[15] Skytek Corp. SkyRead M1-mini - Product reference guide. *Skytek LCC, Colorado, USA*, 2004.

[16] Skytek Corp. Using the Skytek Protocol: RFID Tag Commands. *Application Note 002, Interface Control Document, January*, 2004.

[17] E. Cuellar. The Case for Portable Electronic Health Records. *Journal of AHIMA, September 2004*, September 2004.

[18] Datamonitor. Legal and Regulatory Issues in eHealth Security: An Overview of Europe and the US. *MarketResearch.com*, October 2002.

[19] C. Davenport. Analysis of PDAs in nursing: Benefits and barriers. *University of Phoenix Online, http://www.rnpalm.com*, 2004.

[20] S. Davis. Tagging along. RFID helps hospitals track assets and people. *Health Facil Manege. 2004 Dec;17(12):20-4.*

[21] J. Douglas and S. Larrabee. Bring barcoding to the bedside. *Nursing Management. 2003, May 34(5):36-40.*

[22] Enorgis. Flexible screen technology. *Enorgis, www.enorgis.com*, September 2002.

[23] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. *Selected Areas in Cryptography*, 2001.

[24] J. Geier. Wireless Networking Handbook. *MacMillan Computer Publishing*, 1996.

[25] J. Geier. Deploying WLANs in Hospitals. *Wi-Fi Planet*, August 2003.

[26] M. Gilje, I. Tondel, F. Paint, T. Johannessen, J. Francis, and C. Duranton. Secure Fast Handover in an Open Broadband Access Network using Kerberos-style Tickets. *IFIP International Federation for Information Processing*, 2006.

[27] G. Gruman. 5 Essentials to Wireless Security. *CSO Online*, June 2005.

[28] Hewlett-Packard. HP biometric security toolkit. *White Paper, Hewlett-Packard*, 2003.

[29] HIMSS. 15th annual HIMSS leadership survey. *Health Informatics Management Systems Society*, 2004.

[30] R. Hopkins. Strategic short study – names and numbers as identifiers (final report version 2.0). *CEN/TC 251 Secretariat: SIS-HSS (Swedish Healthcare Standards Institution)*, May 1998.

[31] Texas Instruments. Tag-it HF-I transponder. *Reference Guide*, 2002.

[32] Intel. Transforming Hospital Communications. *White Paper*, 2006.

[33] JCAHO. Sentinel event statistics. *Joint Commission on Accreditation of Healthcare Organisations*, June 2003.

[34] JCAHO. JCAHO: Guidelines for patient safety at hospitals. *Joint Commission on Accreditation of Healthcare Organisations*, 2005.

[35] F. Jossi. Electronic follow-up: Barcoding and RFID both lead to significant goals, efficiency and safety. *Health Informatics. 2004 Nov;21(11):31-3.*

[36] M. Klepal, R. Mathur, A. McGibney, and D. Pesch. Influence of people shadowing on optimal deployment of WLAN access points. *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, Vol.6, Iss., 26-29 Sept. 2004 Pages: 4516- 4520 Vol. 6.*

[37] L. Kohn, J. Corrigan, M. Donaldson, M. Konheim, and H. McAndrew. To Err Is Human: Building a Safer Health System. *Committee on Quality of Health Care in America, Institute of Medicine*, 2000.

[38] S. Krishnamoorthy, J. Reed, C. Anderson, P. Max, and S. Srikanthyayani. Characterization of the 2.4 GHz ISM Band Electromagnetic Interference in a hospital environment. *Mobile and Portable Radio Research Group, Virginia Polytechnic Institute*, 2003.

[39] E. Latorilla. Care2x Hospital Information System. *The Care2x Open Source Project, http://www.care2x.org*, 2006.

[40] A. Lee, M. Leung, and K. So. Managing patients with identical names in the same ward. *Int J Health Care Qual Assur Inc Leadersh Health Serv. 2005l18(1)::15-23.*

[41] EMC legislation and standards in Europe. The EC Medical Devices Directive 93/42/EEC. *Official Journal L169-1993*, 1993.

[42] EMC legislation and standards in Europe. Evaluation of the interaction between wireless phones and hearing aids, phase i: Results of the clinical trials. *EMC Report 1997-2*, August 1996.

[43] EMC legislation and standards in Europe. Medical Equipment Part 1-2: General requirements for safety collateral standard: Electromagnetic compatibility Requirements and tests. *EN60601-1-2*, 2001.

[44] Leuven. The Quality of Health Care/Hospital Activities: Report by the Working Party on quality care in hospitals of the subcommittee on

coordination. *Standing Committee of hospitals of the EU*, September 2000.

[45] R. Lowes. Computer Consult: Towards a handheld EMR. *Medical Economics Archive*, January 2002.

[46] D.C. Medis. HPB No 517: The Electronic Storage of Clinical Records. *The Medical Information System Development Center*, 2002.

[47] Microsoft. Security issues for VPN. *Microsoft Windows TechCenter*, 2005.

[48] Sun Microsystems. RFID enabled system takes patient safety at hand. *Healthcare News, Sun Microsystems*, September 2004.

[49] MSNBC. FDA approves computer chip for humans: Devices could help doctors with stored medical information. *Associated Press*, October 2004.

[50] D. Nadzam and R. Macklis. Promoting patient safety: is technology the solution. *Jt Comm J Qual Improv.*, August 2001.

[51] NEC. Biometrics become part of the healthcare system in the Netherlands. *NEC Security Solutions, NEC (UK) Ltd NEC House 1 Victoria Road London W3 6BL.*

[52] M. Neuenschwander, M. Cohen, A. Vaida, J. Patchett, J. Kelly, and B. Trohimovich. Practical guide to bar coding for patient medication safety. *Am J Health Syst Pharm. 2003 Apr 15;60(8):768:79.*

[53] B. Neuman and T. Ts'o. Kerberos: An Authentication Service for Computer Networks. *IEEE Communications*, 1994.

[54] NOP. Wireless LAN Benefits Study. *NOP World Technology and Behalf of Cisco Systems*, 2003.

[55] F. Ohrtman and K. Roeder. Wi-Fi Handbook: Building 802.11b Wireless Networks. *McGraw-Hill*, 2003.

[56] R. Palmer. *The Bar Code Book*. Helmers Publishing, New York, 1990.

[57] V. Philippov. Working with SIP. *Pocket PC Developer Network, December*, 2001.

[58] P. Phillips, A. Martin, and C. Wilson. An introduction to evaluating biometric systems. *Computer Magazine, IEEE publications*, 2000.

[59] Steinkrug Publications. Wireless Healthcare - Briefing Note. *Steinkrug Publications Ltd, 20 Leaden Hill. Orwell Royston Herts. SG8 5QH*, 2004.

[60] D. Rose. A very Brief History of Paging. *Illinois Signal Communications, Inc.*

[61] B. Saltztein. Bluetooth wireless technology in the medical market. *Code Blue Communications, Inc*, 2001.

[62] SESAM. NETC@RDS Project. *http://www.netcards-project.com/*, 2004.

[63] Siemens. HiMed: The freedom of modern communication. *Siemens HiMed openLine*, 2001.

[64] B. Sokol. RFID in healthcare: Current ROI drivers. *Bradley H. Sokol and Patni Computer Systems Ltd.*

[65] Biocentric Solutions. BioSentry, biometric security for portable applications. *White Paper*, 2002.

[66] M. Sujan, J. Henderson, and D. Embrey. Mismatching between planned and actual treatments in medicine, manual checking approaches to prevention. *Human Reliability Associates*, March 2004.

[67] C. Swedberg. Hospital uses RFID for Surgical Patients. *RFID Journal Inc*, July 2005.

[68] Cisco Systems. Wireless LAN Equipment in medical settings - Addressing radio interference concerns. *White Paper*, 2002.

[69] Cisco Systems. Mobile hospital staff improves productivity and patient care with Cisco wireless solution. *Cisco Systems*, 2005.

[70] Cisco Systems. Cisco Aironet 1200 Access Point. *Product Specifications*, 2006.

[71] K. Takaya, Y. Maeda, and N. Kuwabara. Experimental and theoretical evaluation of interference characteristics between 2.4-GHz ISM-band wireless LANs. *Electromagnetic Compatibility, 1998. 1998 IEEE International Symposium on Volume 1, 24-28 Aug. 1998 Page(s):80 - 85 vol.1.*

[72] Swipe Toolkit. The SWIPE Toolkit, Decode your barcode. *Website: http://www.turbulence.org/Works/swipe/barcode.html.*

[73] L. Versweyveld. Security concerns overhang wireless LANs entry into Europe's hospitals, warns Frost and Sullivan. *Medical IT News, Virtual Magazine Publisher*, November 2002.

[74] Y. Vidal. 101 ways to prevent medical errors. *Medical Management, Lara Publications*, December 2003.

[75] A. Vladimirov, V. Konstantin, A. Gavrilenko, and A. Mikhailovsky. Wi-Foo: The Secrets of Wireless Hacking. *Addison Wesley*, 2004.

[76] J. Wales. The Pocket PC's Prescription for Healthcare. *Pocket PC Magazine*, May 2003.

[77] Wikipedia. iPAQ. *Last accessed*, 2006.

[78] Wikipedia. IPSec. *http://en.wikipedia.org/wiki/IPsec*, 2006.

[79] Wikipedia. Kerberos Protocol. *Last accessed*, 2006.

[80] Wikipedia. Temporal Key Integrity Protocol. *Last accessed*, 2006.

[81] Wikipedia. Transport Layer Security. *http://en.wikipedia.org/wiki/SSL*, 2006.

[82] Wikipedia. Virtual private network. *http://en.wikipedia.org/wiki/VPN*, 2006.

[83] Wikipedia. Windows API. *Last accessed,*, 2006.

[84] Wikipedia. Windows Mobile OS. *Wikipedia, Last accessed*, 2006.

[85] Wikipedia. Wired Equivalent Privacy. *Last accessed*, 2006.

[86] E. Zabrek. The ability of the Pocket or Handheld PC to make medical software accessible on the go will make it the doctor's black bag for the new millennium. *Memorial City-Memorial Hermann Hospital in Houston*, 2003.

COS/CCS 2007-13

www.kth.se