uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Bin Chen

AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Systems Science)

GRADE / DEGREE

Faculty of Graduate and Postdoctoral Studies

FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Handheld Wi-Fi Applications in Ambulance Systems

TITRE DE LA THÈSE / TITLE OF THESIS

Dr. Tet Yeap

DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Dr. Ahmed Karmouch

Dr. Jiying Zhao

Gary W. Slater

Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

HANDHELD WI-FI APPLICATIONS IN AMBULANCE SYSTEMS

BIN CHEN

Thesis submitted to the

Faculty of Graduate and Postdoctoral Studies

In partial fulfillment of the requirements

For the MSc degree in name of

Systems Science

SYSTEMS SCIENCE GRADUATE PROGRAM

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

THE UNIVERSITY OF OTTAWA

Your file Votre référence
ISBN: 978-0-494-49176-8
Our file Notre référence
ISBN: 978-0-494-49176-8

ABSTRACT

This thesis describes the design and implementation of handheld Wi-Fi applications in ambulance systems, which propose a solution that allows ambulance staff to access remote resources in Emergent Medical Services (EMS) from any location, record life measurements on site by using handheld PCs, and transfer patients' life measurements to the Emergency Room (ER) on the way to the hospital. The handheld Wi-Fi applications aim to provide mobility and efficiency for ambulance staff when saving a life.

The handheld Wi-Fi applications afford ambulance staff more flexibility and high performance in accessing and sharing the patient's life data between the ambulance centre and hospitals in time-sensitive circumstances. The handheld Wi-Fi applications provide instant information transportation support for both ambulance staff and healthcare staff. The patient's life measurements are received before the ambulance reaches the hospital.

ACKNOWLEDGEMENTS

I would like to thank the following list of people who supported me during this journey:

- Professor TET HIN YEAP, who sparked my interest in this research and was a great supervisor.
- My family, especially my PARENTS, for instilling in me the passion to learn, and my wife JIANPING MU for her long-lasting understanding and support during the entire project, as well as our coming baby, ISABELLE, for the great happiness and hope she has brought to us.
- My friends and colleagues for their support, love and patience.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

WiFi: Short for *wireless fidelity* and meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, 802.11n, 802.11y, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

CDMA: Short for *Code Division Multiple Access*, a digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence.

1xRTT: Short for *single carrier (1x) radio transmission technology*, a 3G wireless technology based on the CDMA platform. 1xRTT has the capability of providing ISDN-like speeds of up to 144 Kbps. 1xRTT is also referred to as CDMA2000.

SSL-VPN (Secure Sockets Layer virtual private network) is a VPN accessed via HTTPS from any web browser (theoretically), which requires minimal client configuration. SSL is a protocol for managing the security of message transmission on the Internet. It employs the public-and-private key encryption system for managing the security of message

transmission on the Internet. As TLS (Transport Layer Security), a refinement of SSL replaces the earlier protocol, an SSL-VPN is sometimes referred to as a TLS-VPN.

ODBC: short for Open DataBase Connectivity, is a standard database access method developed by SQL Access group in 1992. The purpose of ODBC is to make it capable of accessing any data from any applications, no matter what database management system (DBMS) is handling the data. ODBC inserts a database driver between an application and the DBMS. This layer translates the data queries of the application into commands that the DBMS understands. Both the application and the DBMS must be ODBC-compliant to make this work.

CHAPTER ONE INTRODUCTION

1. 1 Thesis Motivation

When a patient is in an ambulance, every second counts. Minimizing the time required for a patient to receive primary care has always been the concern of the accidents and emergency units. Ambulances are usually the first to arrive on the scene and to administer first aid. However, as the time that it takes to transfer the patient to the hospital increases, so does the fatality rate. In this thesis, handheld Wi-Fi applications in ambulance systems are presented based primarily on third-generation mobile links and on Wi-Fi hotspots around hospitals. This system can be installed inside an ambulance and will permit high-efficiency communications between the moving vehicle and a doctor or a consultant within a base station (usually a hospital). The collected life measurements of patients from medical equipment can be sent to the hospital prior to the arrival of ambulance. The results show that the system can perform satisfactorily in most conditions and can effectively increase the patient's quality of service, while having a modest cost.

WiFi technology could provide time-saving innovations. It gives critical care and professional information instantly with a wireless mobility solution. When an emergency call is

launched, an ambulance is dispatched and the Emergency Medical Services (EMS) is activated, which combines the ambulance centre database, CDMA2000 1xRTT networks, and mobile computing. The ambulance centre database provides vital information on a citizen's medical history, which is instantly transmitted to the ambulance. The ambulance is equipped with a wide-area mobile radio system that includes 1xRTT tracking technology to enable media communication from the ambulance centre to the ambulance. Connecting a wireless access point to an ambulance itself makes it a roaming wireless line. Using wireless-based computing, the handheld PC can now collect critical life measurements, including the pulse, blood pressure, and overall condition (Ambulance Call Report, for instance) of patients. All the information stored in a handheld PC or an ambulance workstation is then transmitted from the patient's site to the wireless local area network (WLAN) system in the hospital, forming an efficient, rapid, and reliable patient care.

1. 2 Thesis Objectives

This thesis aims to analyze the role of mobile computing and how to add wireless technology into the mix of existing technologies for ambulance-hospital communications, and then provide real-time information and data to ambulance-hospital systems. Considering the resources on hand, the design and implementation in this thesis will focus on the information transferred from the ambulance fleet to the hospital using Wi-Fi technology for an experimental prototype.

The system consists of handheld PCs configured to allow EMS personnel to record critical patient information and basic health status variables in the field and transfer such information to the Emergency Room (ER) prior to or upon the patient's arrival. This data will be particularly useful in enhancing emergency care for crash and accident victims.

Handheld computing devices feature a customized software application that allows the user to easily enter the patient's information and health status through a touch-sensitive screen. Data collected on the handheld PC can be transferred to the ER through a wireless transmission, the Wi-Fi technology. The patient's information that was collected is output at the ER in the form of a simple, standard form that summarizes the data collected on the patient in the field. To use the wireless printing utility, ambulance personnel launch the customized printing software on the handheld PC to output the form at a network printer in the ER. In addition to the benefits of patient data exchange, the system helps to streamline the administrative and reporting requirements for pre-hospital care. At the conclusion of each work shift, the data collected on the handheld PCs can be uploaded to the ambulance workstation. By allowing EMS personnel to enter patient data during or between calls, this feature has been shown to increase the accuracy of the data collected, reduce the total time required to complete mandatory reports, and improve the timeliness of report submission.

Many healthcare providers are finding beneficial reasons to install WLANs, mostly to provide mobile network applications to their ambulance centres or hospitals. In fact, ser-

vice providers have begun using the existence of WLAN access as an effective advantage. These ambulance centres are targeting the growing demand of the quick response of ambulance dispatching. Using handheld PCs with embedded super-fast Wi-Fi (802.11b/g/n) technology and CDMA 1xRTT & 1xEV-DO networks, ambulance staff are now able to wirelessly download the latest records of the patient from the ambulance centre database, upload the instant life measurement to hospitals, and constantly keep the direct communications with emergency units. As a result, ambulance centres save more time.

1.3 Thesis Layout

Chapter 2 reviews the traditional ambulance information system and Wi-Fi technology. The next chapter presents the proposed network architecture for advanced ambulance systems. Chapter 4 describes the design and implementation of the prototype of handheld Wi-Fi applications. Chapter 5 concludes this thesis and discusses the future work.

CHAPTER TWO
BACKGROUND

2.1 Traditional Ambulance Information Systems

Traditionally, ambulance services have been regarded mainly as transporters of ill or injured people to hospital. Ambulance crews have, of course, always provided essential and often life-saving interventions at the scene and during the journey to hospital. They usually obtain the demography of the patient, not only in basic life support treatment of emergency patients, but in how to appropriately handle situations that may arise during any phase of operations. This includes, but is not limited to dealing with problematic patients, decision making, MCIs, and interacting with other agencies. They use the ambulance VHF radio to contact the Emergency Department with the following information:

i.) Age and gender

ii.) Chief complaint

iii.) History of chief complaint

iv.) Pertinent past medical history and medications

v.) Pertinent vital signs

vi.) Treatment rendered by this agency and others (i.e. Oxygen by RPI, Signal 600 by TFD)

vii.) Estimated time of arrival

Upon arrival at the medical facility, shut down any nonessential ambulance items (e.g. dome lights, heat or A/C, vent, etc.). Give a report to the appropriate staff member. At the hospital ER, assist the registration clerk in obtaining patient information and try to get a face sheet. Complete paperwork, obtain times and numbers, and notify appropriate dispatch centre(s) that they are available for the next call, using the telephone at the medical facility.

The focus, nevertheless, has been on their function to deliver patients to the hospital, with response standards being the only measure of effectiveness.

One factor that needs to be considered seriously is patient confidentiality. All information regarding to the patient is confidential in nature and not a matter of public record. All requests for patient information must be referred to the corresponding policy. All information is protected in accordance with the Health Insurance Privacy and Portability Act (HIPPA).

Using the traditional ambulance VHF radio has limitations with regard to security. In addition, it lacks efficiency and mobility. The ambulance staff are not able to access remote resources in EMS from any locations and records life measurement on site. They cannot transfer patients' life measurements to the ER in a secured method on the way to the hos-

pital. That is the reason why we are introducing the handheld Wi-Fi applications in ambulance service.

The handheld Wi-Fi applications give ambulance staff more flexibility and high performance in accessing and sharing the patient's life history and life measurement between the ambulance centre and hospitals in time-sensitive circumstances. The handheld Wi-Fi applications provide instant information transportation support for both ambulance staff and healthcare staff. The patient's life measurements are received before the ambulance reaches the hospital.

2.2 Wi-Fi Technology

2.2.1 Wi-Fi Access

Wi-Fi (Wireless Fidelity) offers many advantages over traditional networks. Primarily, the wireless network extends high-speed access across metropolitan areas at significantly lower costs than fibre, copper, or other wireless alternatives. Wi-Fi services can be, and typically are, deployed within days, not months, eliminating last-mile bottlenecks, while accommodating the demand for bandwidth-intensive applications. Wi-Fi networks incorporate encryption and authentication to increase privacy and minimize the potential for fraud. The Wi-Fi network infrastructure provides symmetrical bandwidth upstream and downstream, supplying constant committed bandwidths that are not degraded, even dur-

ing peak periods of traffic volume.

Wireless LAN technology is reshaping the local area networking landscape. Most wireless LANs are based on a set of technologies known by the IEEE 802.11x (where x is a, b, g, or n), or by the open standard Wi-Fi. Wi-Fi technology is the popular term of a high-frequency WLAN, the wireless equivalent of Ethernet, providing seamless connectivity anytime, anywhere. Wi-Fi networks are simple to setup and maintain and provide throughput up to 54 Mbps to date. WiFi 802.11b/g specification allows for the wireless transmission of approximately 11 to 54 Mbps of raw data at distances from several dozen to several hundred feet over the 2.4 GHz unlicensed band. The distance depends on impediments, materials, and line of sight.

It is an extension of Ethernet to wireless communication, and as such, is ecumenical about the kinds of data that pass over it. It's primarily used for TCP/IP, but can also handle other forms of networking traffic, such as AppleTalk or PC file-sharing standards.

In the field, Wi-Fi technology is used to connect hospital-based networks in real time with the ambulance fleet. In the hospital environment, Wi-Fi technology provides a high-speed connection to the local area network. It is used to connect the web application server, the database server, PCs, peripherals such as printers, and other devices such as handheld PCs with a slip-in wireless network card or built-in Wi-Fi through an access

point. Hospital staff can roam throughout their facilities while maintaining a wireless connection to the hospital's WLAN and the Internet.

2.2.2 Up-to-Date Synchronization

Handheld PCs come with several synchronization methods, such as modem, cradle/cable, infrared to PC/handheld, and Wi-Fi. Applying Wi-Fi synchronization to this system, users can access their WLAN and synchronize data with database servers instantly. In addition, they can also print directly to their network printers wirelessly.

2.2.3 Enhanced Security

For mobile applications, users need behind-the-firewall access to their networks and handheld PCs shipped with a built-in PPTP (point-to-point tunneling protocol) virtual private network (VPN). VPN was developed to enable client systems to securely connect to servers over the public Internet. VPN employs strong authentication and encryption mechanisms that have proven extremely robust over the past several years. In addition, VPN is able to create a tunnel between two end points, protecting against intrusion for packets traversing the Internet. This solution enables a secure communication between the handheld PC's applied network.

At the foundation of VPN security is Internet Key Exchange (IKE), a protocol within IP-Sec (IP Security) that provides three authentication methods for protecting data and

communications, being able to encode the header and payload data in packets using key encryption, which can yield communications that defy all but the most determined attacks. Under IKE, packets can be protected using a pre-shared secret key between two parties or using standard public key encryption. IKE also supports the use of digital certificates, which can provide another level of confidentiality when validated by certificate authorities. By deploying a proven VPN security mechanism over 802.11b/g networks, healthcare institution can create a secure connection between wireless clients and the healthcare institution network.

VPN works by establishing one-to-one secure connections between clients and a VPN gateway, which, in the case of 802.11b/g networks, sits just behind the wireless access point. In essence, each client on the network communicates with its access point over a dedicated VPN tunnel. Packets traveling from one client to another over a wireless network first pass through then are sent to one client's VPN gateway. The packets then travel over the wired local network to another VPN gateway, where they are encrypted before being transmitted to the receiving client through a wireless access point. By placing the VPN gateway behind the 802.11b/g access point, the healthcare institution can ensure that all communications that go over the air are protected.

The Wired Equivalent Privacy (WEP) protocol built into 802.11b/g provides a common way to authenticate users and encrypt data. WEP technology provides an encapsulation

technique that scrambles data before it goes over the air and an authentication algorithm called shared key authentication to authenticate the client. Other authentication methods include EAP (Extensible Authentication Protocol) Authentication, Mac address authentication, and MIP (Mobile IP) authentication.

EAP is an extension to PPP. EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in a LAN frame.

In wireless communications using EAP, a user requests a connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication.

After choosing 802.11 authentications for the wireless network, one of the most difficult and important decisions regarding its deployment is to decide which EAP authentication mechanism will be used.

Although EAP supports a group of authentication methods, only four are commonly used.

They are MD5, a one-way authentication of supplicant-to-network using passwords; Cisco's proprietary username-based LEAP (Lightweight Extensible Authentication Protocol), a type of Radius EAP protocol; TLS, which uses PKI-issued (public key infrastructure) digital certificates for strong mutual authentication; and, TTLS, which combines server-side certificates with other authentication such as passwords.

Not every supplicant supports every authentication method defined in 802.11. Not every RADIUS/EAP server supports every method. And not every access point supports all methods. The choice of EAP authentication then drives everything else in your network.

Method	*Description of Most Common Implementation*	*Authentication Attributes*	*WEP Key Generated?*	*Deployment Difficulty*	*Wireless Security*
MD5	Challenge-based password	One-way authentication	NO	Easy	Poor
TLS	Certificate-based two-way authentication	Mutual authentication	YES	Hard	Best
TTLS	Server authentication via certificates; client via other method	Mutual authentication	YES	Moderate	Better

Table 1: Summary of Common EAP Authentication Methods

MD5 Authentication Method

The MD5 authentication method is the simplest one available to wireless LAN users, and support is required in the EAP standard. However, the insecurity of MD5 in a wireless environment is so blatant that some wireless vendors have chosen not to allow MD5 as an authentication method. With MD5 authentication, the authenticator sends a challenge to the supplicant: a string, along with a serial number. The supplicant proves it knows the password by hashing the challenge, the string, and the password together and then sending the information back.

Challenge-based authentication schemes, like MD5, were designed to counter the insecurity of schemes like PAP (Password Authentication Protocol), which actually send the username and password in clear text across the wire. With MD5 (or CHAP in traditional PPP), the password does not pass across the wire. Instead, the supplicant proves that it knows the password. MD5 is fine for dialup, but there are three issues that render MD5 less than optimal for wireless authentication.

First, MD5 requires that user passwords be stored in a way that lets the authenticator obtain the original plain-text password. You will sometimes hear this referred to as "reversibly encrypted." This opens up the possibility of someone other than the authentication server getting access to the file of passwords.

Secondly, MD5 only authenticates the supplicant. It does nothing to authenticate the authenticator, the wireless access point. Since wireless is especially vulnerable to impersonation, this is a major problem. Whereas impersonating a dial-up access server on the other end of a phone line is fairly difficult, impersonating wireless just means getting within a couple hundred feet of the supplicant. This lack of mutual authentication is the reason why some wireless vendors have chosen not to allow MD5.

Thirdly, MD5 does not create a WEP session key. Ideally, immediately after authentication, the wireless client and access point would jump into WEP-encrypted communications, which reduces the risks of eavesdropping, impersonation, or data corruption by a hostile attacker. Other authentication methods, such as TLS and TTLS, support this but MD5 does not, and therefore this limits its usefulness in the wireless world.

TLS (Transport Layer Security) Authentication

EAP (Extensible Authentication Protocol)-TLS is an IETF-standardized authentication method based on the same protocol used for secure Web traffic via the SSL (Secure Sockets Layer) protocol. SSL, as initially developed by Netscape Corporation for use with its Web browsers and servers, is the protocol used by Web browsers and servers to negotiate an encrypted connection. When you use an https:// link, http-over-SSL is invoked, and authentication takes place automatically.

There are very few differences between SSL version 3 (which is supported by all current versions of Web browsers) and TLS. Most people think of SSL (or TLS) largely in terms of the result: an encrypted session between your browser and the Web server. But as part of setting up the session, SSL starts with an authentication phase, and that is what is being used in any EAP-TLS operation.

TLS authentication within EAP is very simple. You take the TLS session establishment dialog between the supplicant and the authentication server and pack each TLS message inside of an EAP-TLS packet. When the TLS authentication dialog succeeds, the authenticator is informed, and access to the network is granted.

Although TLS has actually set up an encrypted channel between the authentication server and the supplicant, this channel is not used --- the supplicant wants to talk to the authenticator, not the authentication server. Instead, a piece of the keying material created during the TLS session establishment for that channel is sent to the authenticator. Then, the supplicant (which already knows the TLS-established secret key) and authenticator use that key for WEP encryption.

In EAP-TLS, certificates are used to authenticate the authentication server to the supplicant, and, optionally, to authenticate the supplicant to the authentication server. The authentication server starts by sending its digital certificate to the supplicant. The most

common authentication used today on the Web with SSL is one-way authentication-a server sends its certificate to your browser to prove its identity. However, with EAP-TLS, you are more interested in mutual authentication so that you can protect your network against man-in-the-middle attacks.

The advantages of EAP-TLS make it a preferred authentication method. Both wireless client and access points are strongly authenticated using digital certificates. As a side effect, a per-session WEP key is set up, and the client can be re-authenticated and re-keyed as often as needed without inconveniencing the end user at all.

The problem with EAP-TLS is that it requires that clients hold digital certificates. While many enterprises have deployed a PKI infrastructure to handle certificates, many other enterprises are not ready for that. Some have also decided that other authentication systems, such as token-based authentication, align more closely with their business models and security policies. In addition, not all RADIUS servers that support EAP also support the TLS authentication method.

TTLS (Tunneled TLS) Authentication Method

Healthcare institutions that want the security of TLS, but have legacy authentication methods or token-based authentication methods will probably choose TTLS for their EAP method.

EAP-TTLS is essentially an extension to EAP-TLS. The authentication in EAP-TLS is typically mutual. Both parties authenticate each other. EAP-TTLS authentication uses certificates to authenticate the server side, and a simpler method to authenticate the client side, all the while maintaining similar security properties to TLS, such as mutual authentication and a shared secret for session WEP key. In fact, EAP-TTLS is actually better than EAP-TLS in at least one way. An eavesdropper cannot even see the user identity, because it is sent only after the TLS tunnel is established.

EAP-TTLS accomplishes this by packing another authentication protocol inside of the TLS tunnel when it comes time to authenticate the user. That is where the "Tunneled" in "Tunneled TLS" comes from. The network manager has the option of using a very simple tunneled authentication protocol, such as clear-text passwords or challenge-response passwords, or a more advanced technique, such as token-based authentication.

The main drawback of EAP-TTLS is that the Internet community has not yet reached an

agreement on this as the best approach for environments where digital certificates are not available. Another proposal being considered by the IETF is PEAP (Protected EAP), which solves many of the same problems as EAP-TTLS.

2.3 CDMA 1xRTT

CDMA 1xRTT stands for Single Carrier(1x) Radio Transmission Technology, a 3G wireless technology based on the CDMA platform and that is part of the CDMA2000 family of protocols. 1xRTT has the capability of providing ISDN-like speeds of up to 144 Kbps. 1xRTT is also referred to as CDMA2000, which includes successors to 1xRTT such as Single Carrier Evolution Data Only (1xEV-DO). It is built on top of the CDMA-based mobile phone networks and allows for ISDN-like data transfer speeds up to 2400 kbps (1xEV-DO is capable of much higher speeds). Sprint's PCS Vision and Verizon's Express Network use this technology. As of this writing, Verizon Wireless is experimenting with 1xEV-DO in two U.S. markets, with testers obtaining data rates between 500 and 800 kbps.

2.4 EMS

EMS (Emergency Medical Service) is responsible for operating and dispatching a fleet of ambulances and first-aid staff for a variety of emergency situations. EMS combines 1x RTT networks and a customized tracking system to allow EMS to know the exact loca-

tion and status of each of the ambulances at any given time, past or present. Along with position information, additional data such as speed is also gathered and transmitted wirelessly back to the ambulance centre. This powerful function enables EMS to optimally operate, dispatch, and manage ambulances to minimize response time and help save lives. Working with the EMS CA server, only authorized requests can be granted access to the ambulance centre database.

CHAPTER THREE

PROPOSED NETWORK ARCHITECTURE FOR ADVANCED AMBULANCE SYSTEMS

3.1 System Architecture

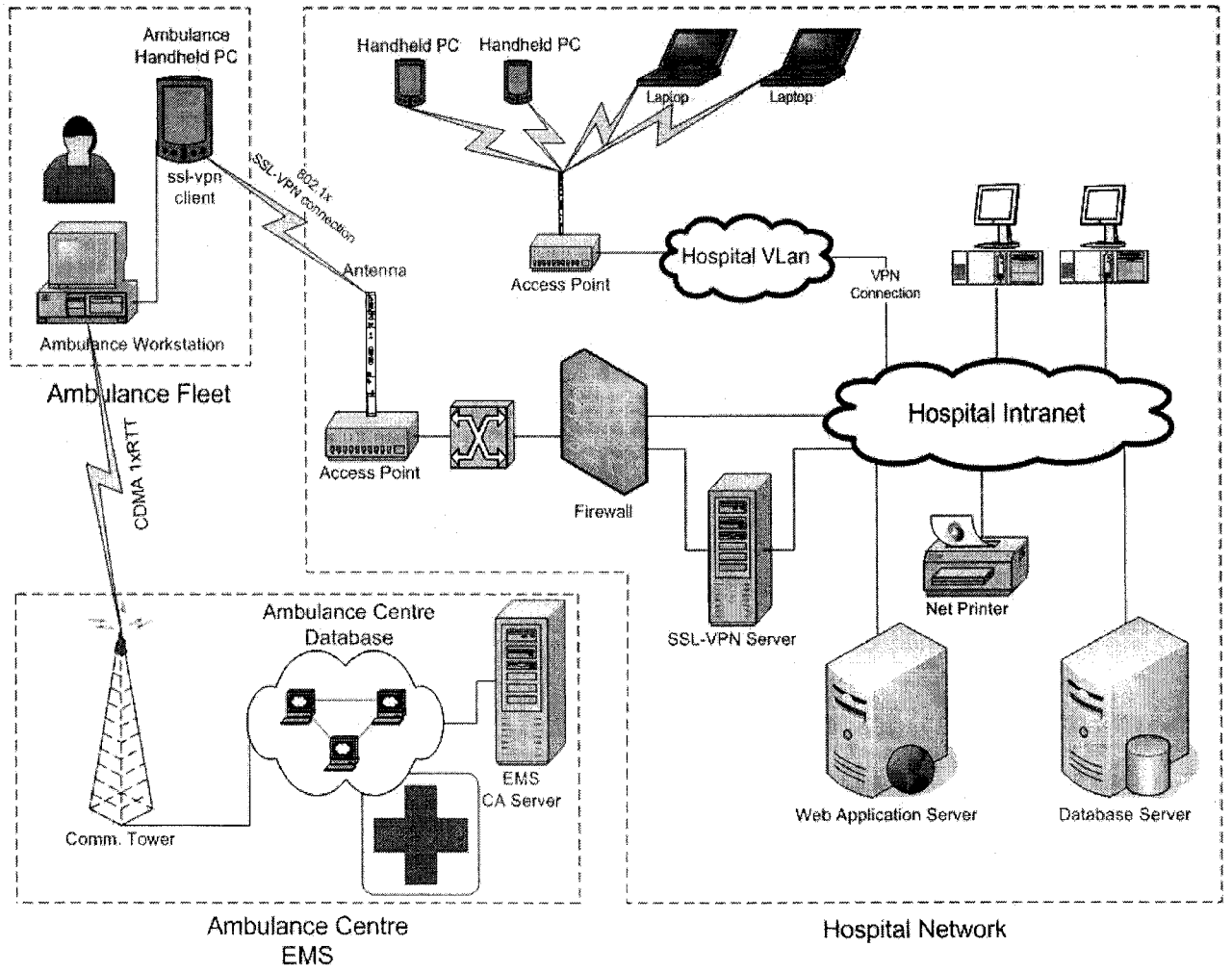


Figure 1: Advanced Ambulance Systems

The proposed network architecture for advanced ambulance systems consist of three main components: the ambulance centre EMS enabled with the EMS CA server and a CDMA 1xRTT WAN connection; the ambulance fleet equipped with Wi-Fi enabled handheld PCs and a SSL-VPN connection; and the hospital network, including the web application server and the database server secured by the SSL-VPN server.

As described in the structure graphic, the ambulance staff can use a handheld PC to securely communicate with the web application server on the hospital intranet. The ambulance staff input the patient's information into the handheld PC, which includes the admission information, the clinical information, and the physical exam records. When the Wi-Fi connection is recognized and established, the history record from the ambulance centre EMS and the life measurement of patients will be uploaded to the web application server on the hospital intranet through the SSL-VPN channel after the identity authenticated by the SSL-VPN server.

The web application server then recognizes the patient's information and saves it in the database server. Furthermore, the web application server analyzes the patient's information, indexes the ER group that the patient's information should be sent to, sends the patient's information to the recipients, and prints out the information through the dedicated network printer.

The recipients in the hospital system include the nurse station, the on-duty doctors, and the specialist in a particular medical field for a certain patient. The patient's information is sent to the

nurse station at the ER or the operation room if necessary. The system is capable of printing the patient's information on the printer at the nurse station. The on-duty doctors in the ER or the specialist at the operation room will be able to review the patient's information with the printout copy at the nurse station or the email application on their handheld PCs.

3.2 System Components

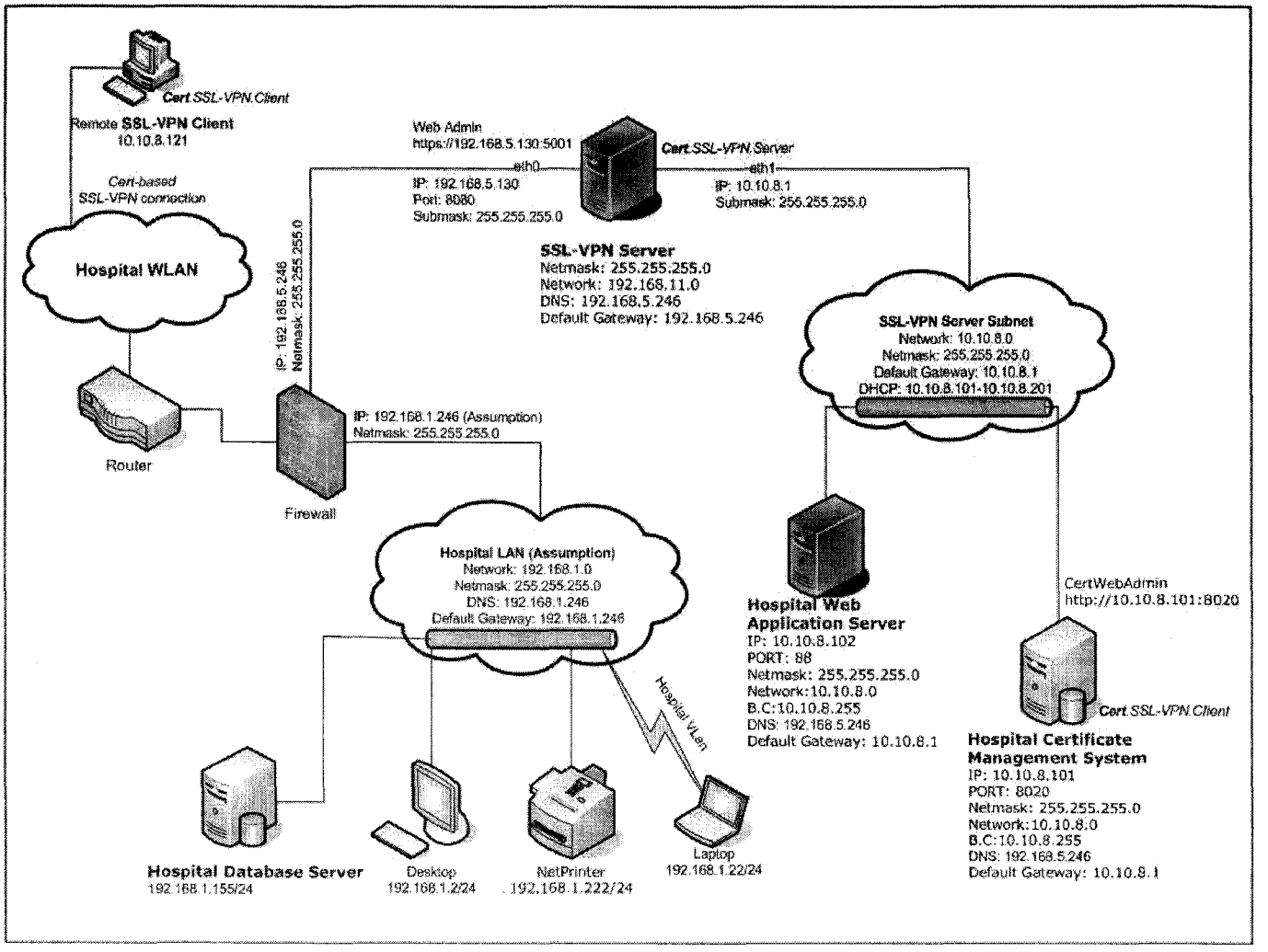


Figure 2: SSL-VPN Network Architecture

3.2.1 SSL-VPN Server/Client

Secure Sockets Layer (SSL) has emerged as the leader in the remote access VPN space. Analysts and the press are giving more attention to SSL VPN than ever before. SSL is a commonly used protocol for managing the security of a message transmission on the network. SSL works by using

a public key to encrypt data that is transferred over the SSL connection. SSL is a higher-layer security protocol, sitting closer to the application. This close connection to application layers means that SSL can easily provide the granular access control that remote access and extranet VPN require.

SSL-VPN uses SSL and proxies to provide authorized and secure access for ambulance staff to the web application server, as well as other resources. SSL-VPN delivers user-level authentication, ensuring that only authorized ambulance staff have access to the specific resources, as allowed by the hospital's security policy or access control. SSL-VPN enables doctors to securely access patient records from any authorized computer, handheld PC, or dedicated network printer, not just their own PC. SSL-VPN provides a secure connection to the web application server that the ambulance staff is authorized to access. As a result, users never have a direct network connection to the resource they are trying to access.

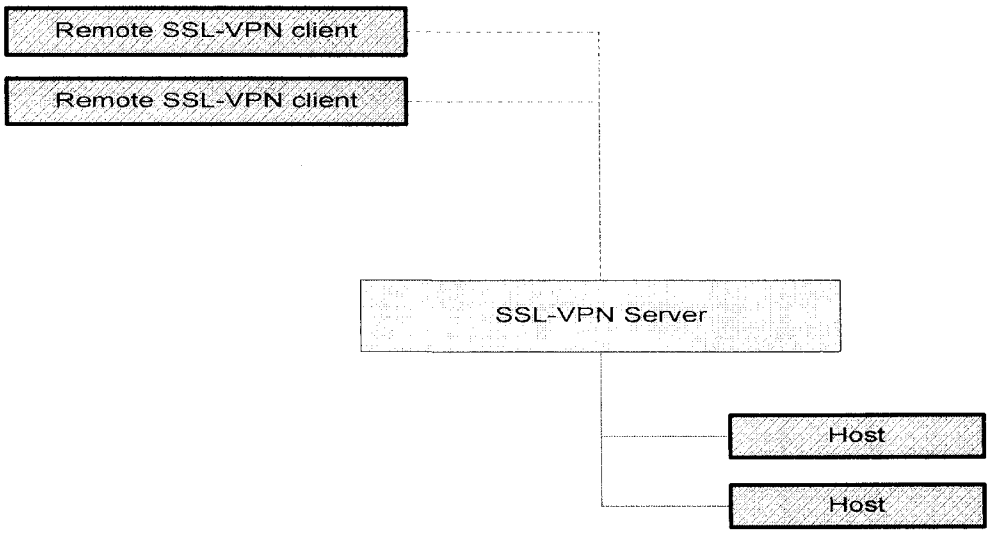


Figure 3: SSL-VPN Server/Client

In this proposed SSL-VPN network, the SSL-VPN server assigns a private IP to remote SSL-VPN clients. A SSL-VPN connection is established between remote the SSL-VPN clients and SSL-VPN server. Remote SSL-VPN clients and the local hosts (web application server, Certificate Management System) are on the same subnet.

3.2.2 Web Application Server

The web application server will be developed on the LAMP (Linux +Apache+ MySQL+ PHP) web server. The main goal of the web application is to read the patient's information, which the ambulance staff has uploaded through a wireless SSL-VPN connection, and write it into the database on the web application server. Once the patient's information is collected in the database, the hospital caregivers can access, email, and print out this data as needed. Furthermore, this data can eventually be transferred to the hospital's local database if necessary. To ensure proper implementation of the web application, the LAMP web application server should be configured as Apache 2.0 + MySQL 5.0 + PHP 5.2.2. The database will be created on the local host, and the following table is to be created in the database with storage engines = InnoDB.

Table comments: InnoDB free: 10240 kB

Field	Type	Null	Default
id	bigint(20)	No	
UploadTime	timestamp	No	CURRENT_TIMESTAMP
Surname	varchar(200)	Yes	NULL
Given Name	varchar(200)	Yes	NULL
Gender	varchar(200)	Yes	NULL
Mail address	varchar(200)	Yes	NULL
City	varchar(200)	Yes	NULL
Province	varchar(200)	Yes	NULL
Post Code	varchar(200)	Yes	NULL
Hospital Registry Number	varchar(200)	Yes	NULL
Date of Birth (YMD)	varchar(200)	Yes	NULL
Health Card Number	varchar(200)	Yes	NULL
Pickup Location	varchar(200)	Yes	NULL
Sending Hospital	varchar(200)	Yes	NULL
C.T.A.S	varchar(200)	Yes	NULL
Skin Temp	varchar(200)	Yes	NULL
Blood Pressure	varchar(200)	Yes	NULL
Heart beat rate	varchar(200)	Yes	NULL
Breath Sounds	varchar(200)	Yes	NULL
Warning System	varchar(200)	Yes	NULL

Indexes:

Keyname	Type	Cardinality	Field
PRIMARY	PRIMARY	0	id
Surname	INDEX	0	Surname

Space usage:

Type	Usage	
Data	16,384	B
Index	16,384	B
Total	32,768	B

Row Statistics:

Statements	Value
Format	Compact
Rows	0
Next Autoindex	5
Creation	May 07, 2007 at 10:17 AM

Figure 4: Database Structure

The implementation of the web application is defined as the following two phases:

3.2.2.1 Uploading patient information

The patient's information will be automatically uploaded as soon as the SSL-VPN connection between the handheld PC and the web application server is established through the hospital WLAN. The web application will save the collected patient information on the web server. The web application is capable of verifying the completion of the data uploaded on the web application server. And it also uses session parameters to ensure that there is only one file uploaded through the same handheld PC in one conversation session.

3.2.2.2 Reading patient information

After the file from the handheld PC is saved on the web application server, the web application will read the file, analyze the file, and save the patient information into the database as shown below:

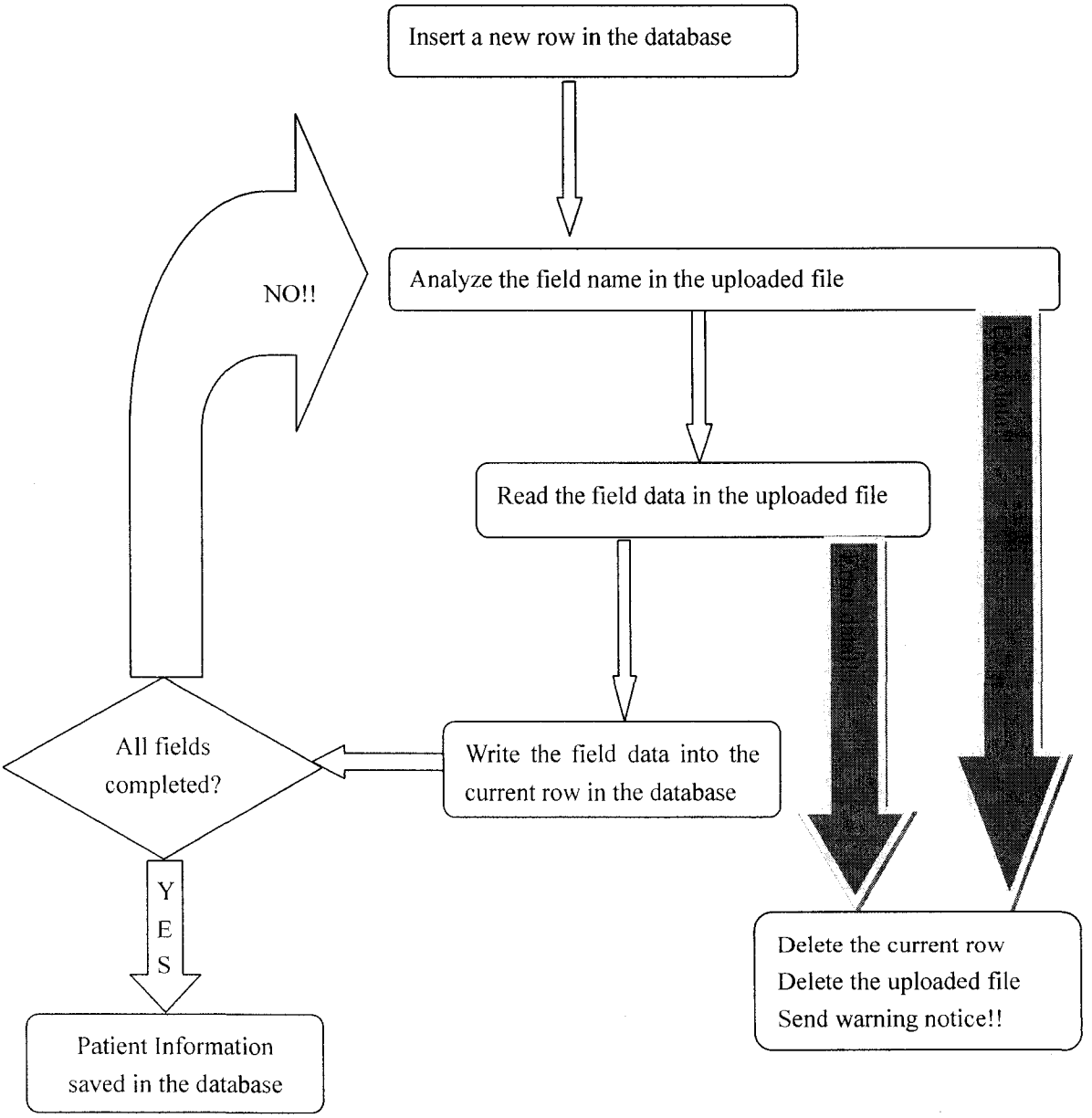


Figure 5: Patient Information Reading & Storing

Here are some considerations we need to discuss regarding reading and storing patient information.

- As the figure shows above, the file of patient information has been uploaded on the web server. We do not need to consider the completion of the file we are reading. Once we check that the file format is not valid, the uploaded file is to be removed, and a warning notice will be returned to the sender.

- We assume that the patient information is valid when the handheld PC holder discovers and saves it into the handheld PC. We are able to find all field names in sequence in the uploaded file. When the web application cannot find the field name in sequence, the web application will automatically delete the input (includes all filed data in the current row in the database and removes the saved file on the server) and rollback the transaction in the database.

- Practically speaking, we use the common expression to analyze the validity of a string in the uploaded file saved on the web application server. If any uncertain strings (e.g. ‘, “, @) are contained in the text file, the web application will automatically delete the input (includes all filed data in the current row in the database and removes the saved file on the server) and rollback the transaction in database.

In addition, the clarification for all feasible faults should be done as much as possible in reading

the patient information unless it is a professional error made by the handheld PC holder. It is a critical and complicated task for the web application service, and will be discussed in detail in the programming process.

3.2.3 Handheld-Based Applications & Database

The record layout of patient information in the handheld PC will be designed based on the form called "ambulance call report" developed by the Ministry of Health and Long Term Care (Ontario), which consists of patient information, clinical information, and the physical exam. The form is shown in the Appendix.

CHAPTER FOUR

DESIGN AND IMPLEMENTATION A PROTOTYPE OF HANDHELD WI-FI APPLICATIONS

The system consists of handheld PCs configured to allow EMS personnel to record critical patient information and basic health status variables in the field and transfer such information to the ER prior to or upon patient arrival. This data will be particularly useful in enhancing emergency care for crash and accident victims.

The handheld computing devices feature a customized software application that allows the user to easily enter patient information and health status through a touch-sensitive screen. The data collected on the handheld PCs can be transferred to the ER through an authorized and secure wireless transmission. The patient information that was collected is then output at the emergency room in the form of a simple, standard form that summarizes the data collected on the patient in the field. To use the wireless printing utility, EMS personnel launch the customized printing software on the handheld PC to output the form at the network printer in the ER. In addition to the benefits of patient data exchange, the system helps to streamline the administrative and reporting requirements for pre-hospital care. At the conclusion of each work shift, the data collected on the handheld units can be uploaded to an ambulance workstation, then synchronized with the EMS database when the ambulance returns to the am-

bulance centre. By allowing EMS personnel to enter patient data during or between calls, this feature has been shown to increase the accuracy of the data collected, reduce the total time required to complete mandatory reports, and improve the timeliness of report submission.

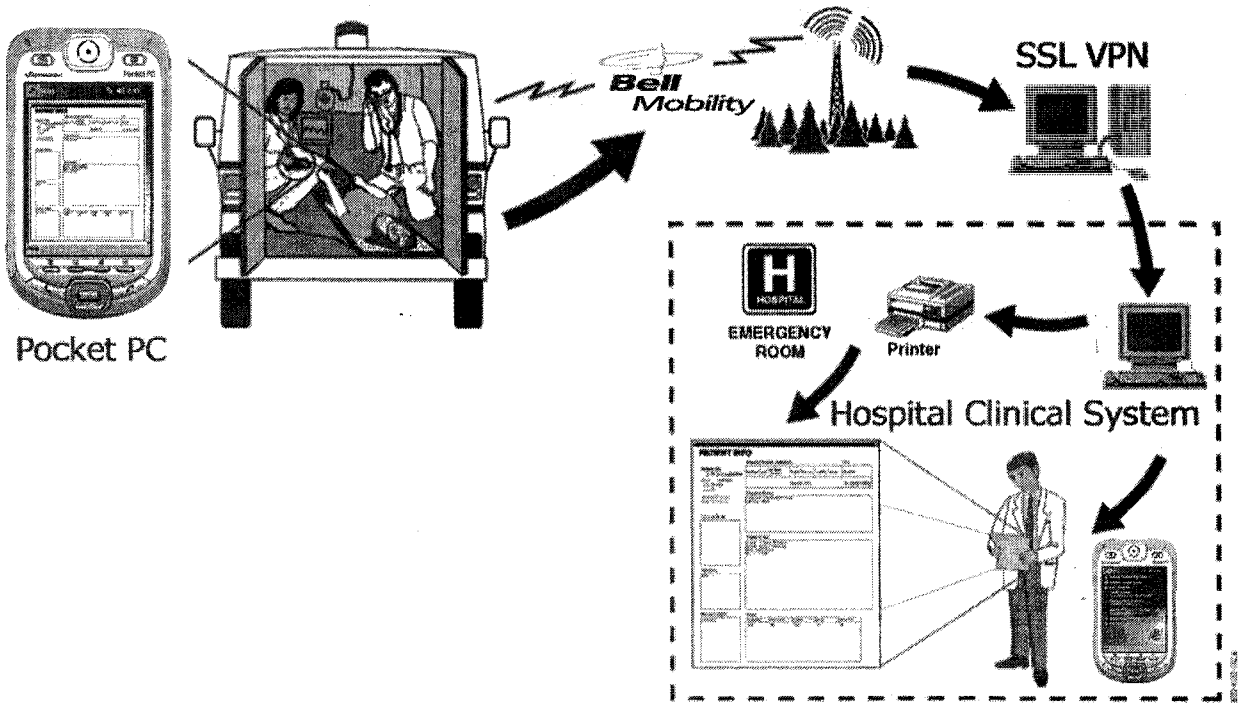


Figure 6: Wireless Handheld Device Assisting Emergency Medical Field Personnel

4.1 Handheld-Based Ambulance Call Report Design

The handheld-base ambulance call report design is based on the form called "ambulance call report" developed by the Ministry of Health and Long Term Care (See appendix 1, appendix 2, and appendix 3), which consists of patient information, clinical information, and the physical exam.

The record layout of ambulance call report on handheld PC features user-friendly interface which facilitates the data input for ambulance personnel. Each record of patient information includes user information, pickup information, clinical information, and physical exam. The user information contains health card number, surname, given name, address, city, province, postal code, hospital registration number, birthday, and version number. The pickup information has health card number, pickup location, pickup code, sending hospital, and time stamp. The clinical information consists of health card number, incident history, medication, allergies, treatment prior to arrival, cardiac arrest information, and time stamp. The physical exam comprises general appearance, head/neck, chest, abdomen, back/pelvis, extremities, and time stamp. Figure 7 shows the record layout in detail.

Because of the uniqueness of health card number of patients, it is set to be the primary

index for each patient record. Time stamp, as the secondary index for each patient record, is critical when the specific date information is needed for the same patient.

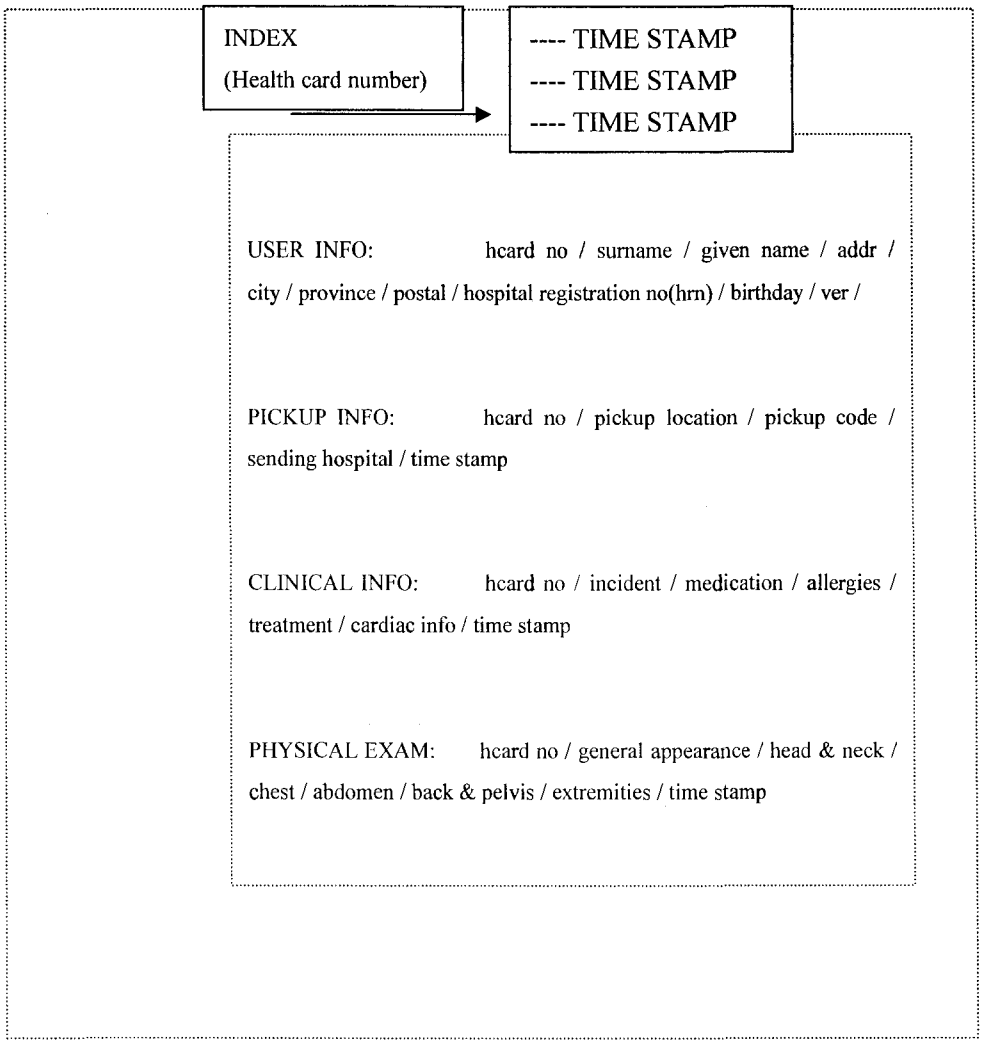


Figure 7: Handheld-Based Ambulance Call Report Design

4.2 Database System Utilizations

Database system utilizations consist of two aspects: database server utilization and handheld-based database utilization.

Transmitting patient data to handheld PC via 1xRTT tracking system, creating recurring report, helicopter transport review, providing billing agencies with patient care data, creating monthly detailed general and treatment guideline audits, and assessing improvements in patient care are the main features of database server utilization.

Handheld-based database utilization includes the following functions: collecting patient care data, transferring patient care record to the database server on hospital web application server via secure wireless LAN, printing readable patient care record, and ***HotSync*** wirelessly synchronizes care data between handheld PCs and ambulance workstation database. In this thesis, the design and implementation of handheld-based database on Palm operating system and pocket PC operating system are both considered. Therefore, the Palm-based database and pocket PC-based database will be discussed in section 4.3 and section 4.4, respectively.

4.3 Palm-Based Database

The interface of Palm-based database provides ambulance staff with a familiar means of accessing and cataloging patient records and setting properties for each patient record they create. Patient records can also be easily viewed, edited, filtered, sorted, and searched whenever needed. With the feature of Open Database Connectivity (ODBC), patient information on handheld PC can transfer to or from other ODBC-enabled database applications.

Figure 8 to figure 21 show the Palm-based database layout and the process of data input in detail. The ambulance staff opens a database named AmbulanceCallReport displayed in Figure 8. HospitalList database can also be edited to add new hospital information as shown in Figure 9 and Figure 11. Figure 10 illustrates the patient information synchronized from the EMS database. The ambulance staff can get the health card number, the name of the patient, mailing address, and hospital code. Figure 12 displays the facility name of the hospital where the patient was sent previously, as well as the address and contact number of that hospital. Figure 13 to Figure 19 let the ambulance staff updates the patient information, including health card number, surname, given name, address, city, province, postal code, hospital registration number, birthday, pickup location, sending hospital, and occurrence time. In Figure 20, the ambulance staff is able to choose the

name of the hospital the patient will be sent to, for example Riverside Hospital. After updating all the information, the ambulance staff draws his/her signature to finish this on-site record shown in Figure 21.

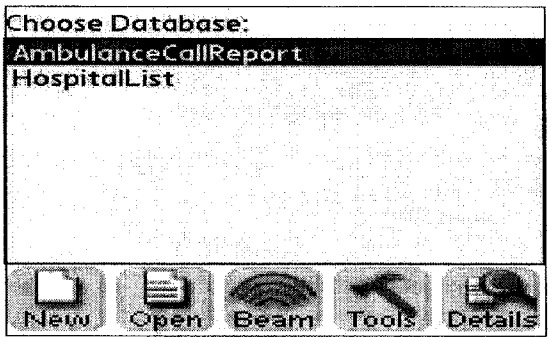


Figure 8: Palm-Based Database 1

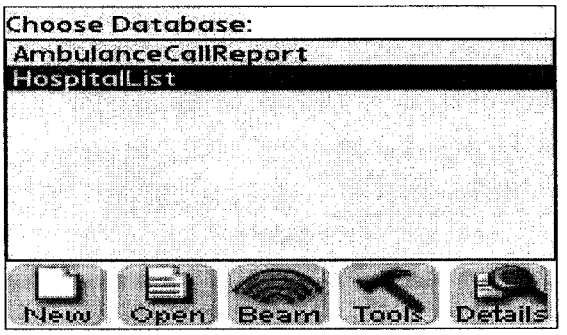


Figure 9: Palm-Based Database 2

Figure 10: Palm-Based Database 3

Figure 11: Palm-Based Database 4

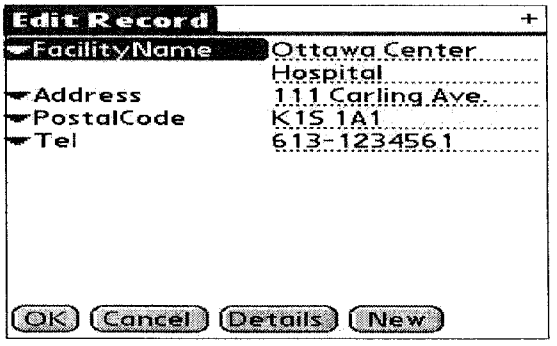


Figure 12: Palm-Based Database 5

Figure 13: Palm-Based Database 6

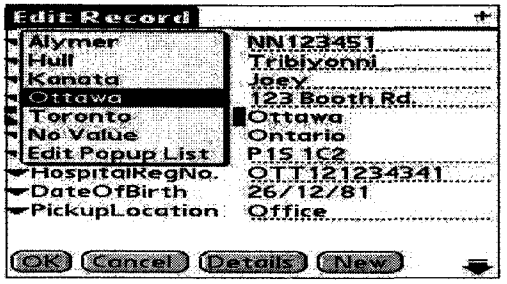


Figure 14: Palm-Based Database 7

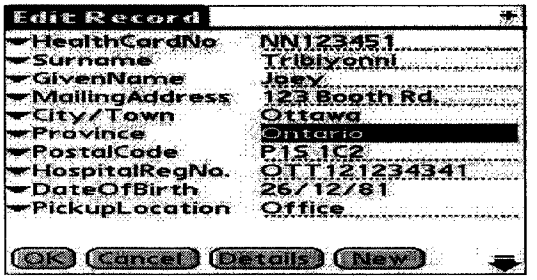


Figure 15: Palm-Based Database 8

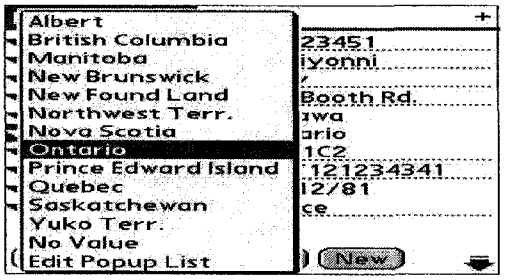


Figure 16: Palm-Based Database 9

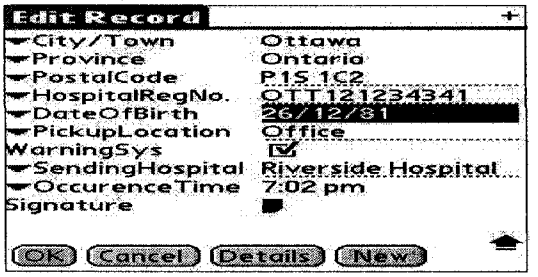


Figure 17: Palm-Based Database 10

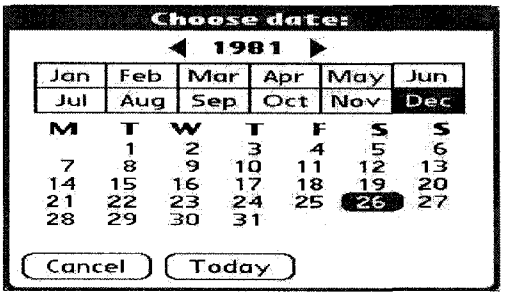


Figure 18: Palm-Based Database 11

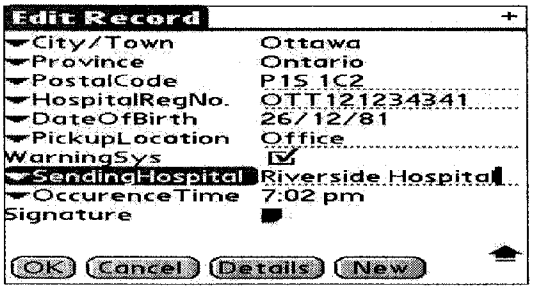


Figure 19: Palm-Based Database 12

Figure 20: Palm-Based Database 13

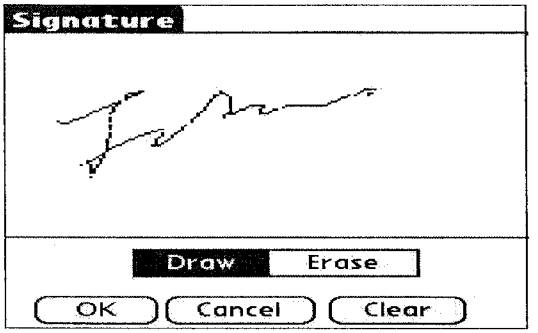
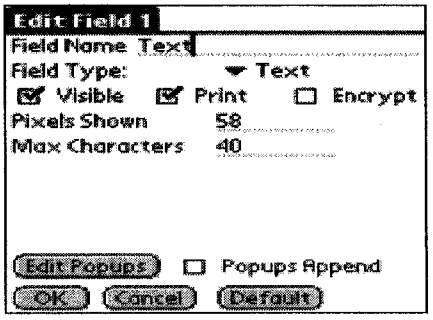


Figure 21: Palm-Based Database 14

4.3.1 Field Properties

Palm-base database field properties are based on the following descriptions:

- **Text Fields**



This diagram shows multi-line text input fields with popups for the most common values. This is the most common type of field. When selected, the following options appear:

Visible

Check if you want this field to be visible on the Edit Record screen.

Uncheck if you wish to hide it on the Edit Record screen.

Print

Check if you want this field to be exported to the memo pad or printed when any of these options are selected: Export Record or Records, Print Record or Records from the Edit Record or the List View screen, respectively. Uncheck if you do not wish to export or print this field.

Encrypt

Check this option if you want the ability to encrypt this specific field. You will need to specify what level of encryption you would like in the security settings before this will become active.

Uncheck if you do not wish to enable encryption for this field.

Pixels Shown

Choose the number of pixels in width that will be shown on the List View screen. There is a maximum of 160 pixels in width on the screen for Palm OS handheld users and a maximum of 240 pixels for Pocket PC users. Setting it to 0 will hide this field on the List View screen. The desktop will display the fields in proportion to the size that is set.

Max Characters

Choose the maximum number of characters allowed for this field. The range is from 1 to 254. This will limit the size of the string allocated for this string when editing it in the Edit Record screen. This can be changed at a later time if you feel you need more room. It only affects the RAM requirements during the editing of a field.

Edit Popups

Here you will be brought to the Edit Popup List screen where you can choose the possible

values for this field.

Popups Append

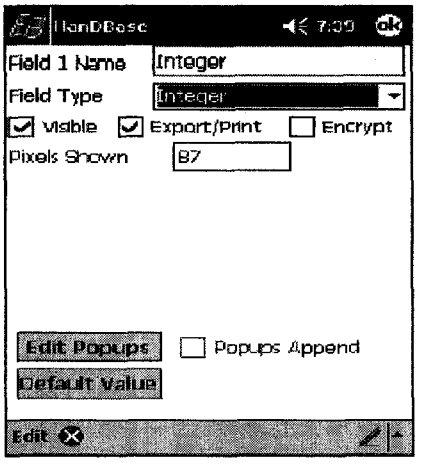
Check this box if you would like the values selected from the popup list for this field to append to the end of any existing value.

Uncheck this box if you would rather the popup value replace the current text value. Checking this option is useful if you would like to allow multiple popup values in a text field. An example of this may be a link to a web site, where you could have http://, www., and .com as popup values, and you would be able to add these on, one by one, to the existing field.

Default

Tap this button to be able to set a default value for this field when a new record is created. There are two options. The first is to use the value from a specific field from a previous record. The second is to use a static value for each and every record.

- **Integer Fields**

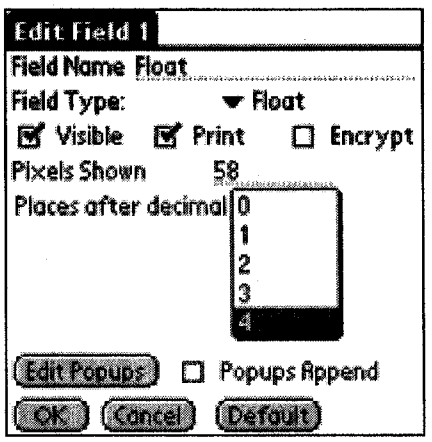


Numeral values with popups for the most common values. This is different from the Text field, mainly in the sorting of entries and that its popups can be numerically sorted. HanDBase can support whole numbers from - (negative) 2147483647 to + (positive) 2147483647. Negative numbers are indicated by the - (minus) symbol. Positive numbers have no symbol. If a number larger or smaller than the allowed number is entered, the user will be notified that it will be set to the greatest or smallest number available. When selected, the following options appear:

Visible/Print/Encrypt/Pixels Shown/Edit Popups/Popups Append/Default

(See Application Manual for details)

- **Float Fields**



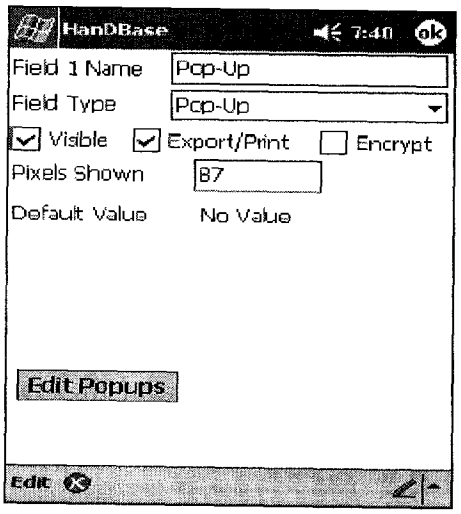
This image shows floating point values with popups for the most common values. This is different from the Integer field in that the numbers can have a decimal point or comma in them. The handheld operating system preferences are used to determine what decimal indicator is used. Palm OS users will find this under the Numbers setting in the Palm OS system Preferences, under Formats. Pocket PC users will find this on the System tab of Settings by selecting Regional Settings. The HanDBase Desktop has its own preference for this in order to properly support the handheld. This option is available by selecting Preferences from the File menu in the HanDBase Desktop application. This field is commonly used for money amounts. HanDBase can support whole numbers from - (negative) 2147483647.9999 to + (positive) 2147483647.9999. Negative numbers are indicated by the - (minus) symbol. Positive numbers have no symbol. If a number larger or smaller than the allowed number is entered, the user will be notified that it will be set to the greatest or smallest number available. The number of spaces after the decimal point or

comma is determined by the settings for the field. When selected, the following options appear:

Visible/Print/Export Record/Encrypt/Pixels Shown/Edit Popups/Popups Append/Default

(See Application Manual for details)

- **Popup Fields**

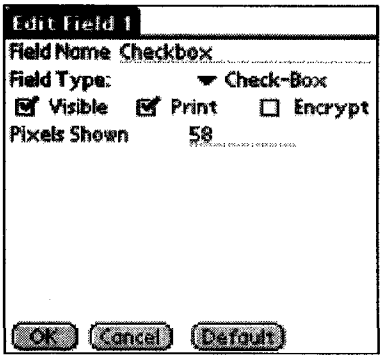


This field type will pop up a list of choices when selected. This differs from the other fields that have popup lists in that the value can only be one of the popup choices (i.e., the user cannot write in any value). When selected, the following options appear:

Visible/Print /Encrypt/Pixels Shown/Default Value/ Edit Popups

(See Application Manual for details)

- **Checkbox Fields**

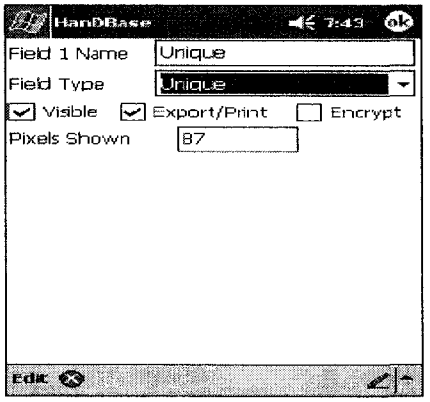


This diagram shows a checkbox for its value, which can be checked or unchecked. When selected, the following options appear:

Visible/Print/Encrypt/Pixels Shown/Default

(See Application Manual for details)

- **Unique Fields**



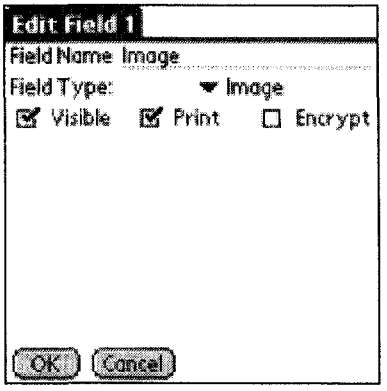
This handheld is automatically filled with a value unique to that record. ***NOTE:*** If you

are using a database that contains a unique field in a multi-user environment, with the HanDBase Sync Exchange add-on or in a single user desktop/handheld solution, this value is not guaranteed to be unique. When selected, the following options appear:

Visible/Print/Encrypt/Pixels Shown

(See Application Manual for details)

- **Image Fields**

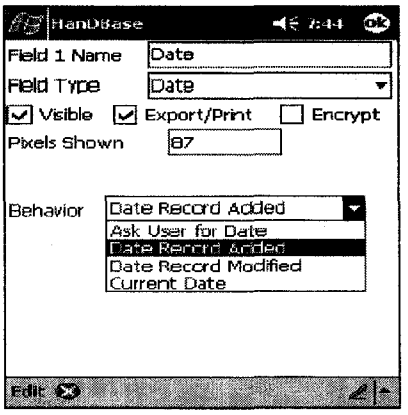


You can capture a pen-drawn image or handwritten signatures using this field type. When selected, the user is taken into a canvas type Edit Image screen, where they may sketch out their image with the stylus. When selected, the following options appear:

Visible/Encrypt

(See Application Manual for details)

- **Date Fields**

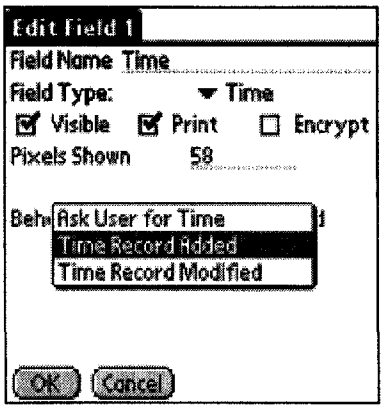


This field type enables you to enter a date. The format of the date on the handheld is dependent on the operating system preferences. Palm OS handheld users will find this under the Preferences tool by selecting Formats. Pocket PC users will find this under the Settings Tools by selecting Regional Settings from the System tab. The format of the date in the HanDBase Desktop for Windows is set in the preferences, to ensure compatibility with the handheld. These settings are accessed by selecting Preferences from the File menu in the HanDBase Desktop. Date fields in HanDBase can have a minimum date of 1/2/1904 and a maximum date of 12/31/2031. If the date is set to 1/1/1904, a value of No Date will be displayed. When selected, the following options appear:

Visible/Print/ Export Record/Encrypt/Pixels Shown/Date Behavior

(See Application Manual for details)

- **Time Fields**

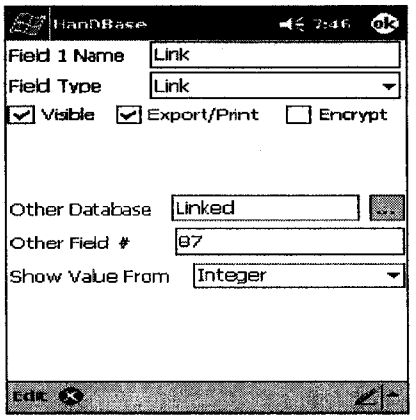


This field type enables you to enter a time. The format of the time is dependent on the handheld operating system preferences. Palm OS handheld users will find this under the Preferences tool by selecting Formats. Pocket PC users will find this under the Settings Tools by selecting Regional Settings from the System tab. The format of the time in the HanDBase Desktop for Windows is set in the preferences to ensure compatibility with the handheld. These settings are accessed by selecting Preferences from the File menu in the HanDBase Desktop. When selected, the following options appear:

Visible/Print/Encrypt/Pixels Shown/Time Behavior

(See Application Manual for details)

- **Link Fields**

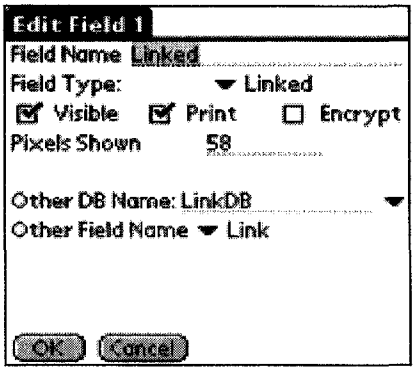


This serves as the starting point for linking two databases together. The Link field will display a button with the field name in it. When pressed, the program will switch to the database specified below. The database, however, will only show the records that were added through the current record in the first (linking) database. This is useful to add sub-records of a different type to individual records. When you are finished adding or editing these linked records, you can tap the button to return to the previous database. For example, a doctor may have a database of patient information, which would include a link field that linked to a Visit database. When the 'Visit' link button is pressed under a patient record in the patient database, the Visit database would be switched to, and would only show the visits that patient had made. When selected, the following options appear:

Visible/Print/Export Record/Encrypt/Other Field Nam&Number/Other Database/ Name&Number/Other Database Name Parameter/Show Value From

(See Application Manual for details)

- **Linked Fields**

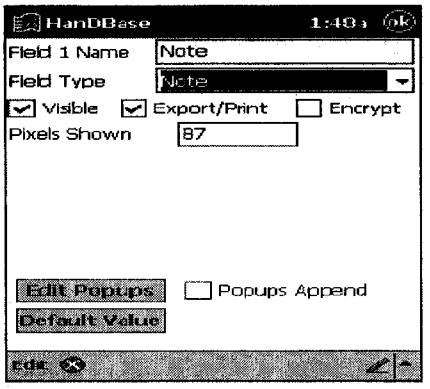


This serves as the landing point for linking two databases together. The Linked field is the field in the second database that will link the two databases together. This field is required in a database that is linked by another database via the Linked field. When a Linked field is pressed in the Edit Record screen, the record in the Other Database Name that it belongs to will show on the screen highlighted. You can reassign this record to another record by selecting another record or just return without selecting another by pressing the button. In addition, when the linked field is visible, it will show the field specified in the other database's link field's Show Value From setting. When this field is selected, the following options appear:

Visible/Print/Export Record Encrypt/Pixels Shown/Other Database Name/Other Field/Name&Number

(See Application Manual for details)

- **Note Fields**

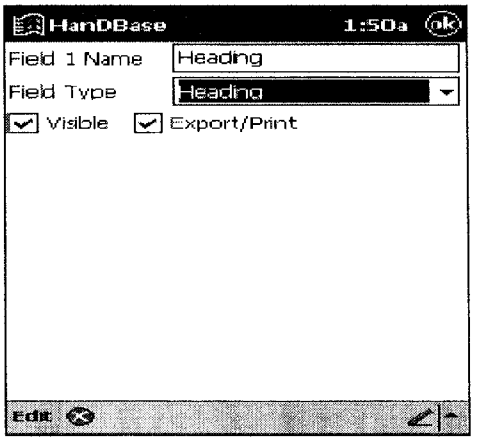


These fields allow for memopad-type notes (up to 2,000 characters in length) and a popup to insert common phrases, words, etc. When selected, the following options appear:

Visible/Print/Export Record/Encrypt/Pixels Shown/Popups Append/Default

(See Application Manual for details)

- **Heading Fields**

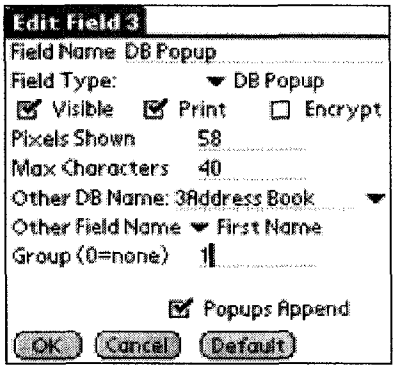


Organize sections of your database with a bold, centre heading. This field actually does not hold any value, but is used for organizational purposes only, when in the Edit Record screen. When selected, the following options appear:

Visible Check if you want this field to be visible on the Edit Record screen.

Uncheck if you wish to hide it on the Edit Record screen.

- **DB Popup Fields**

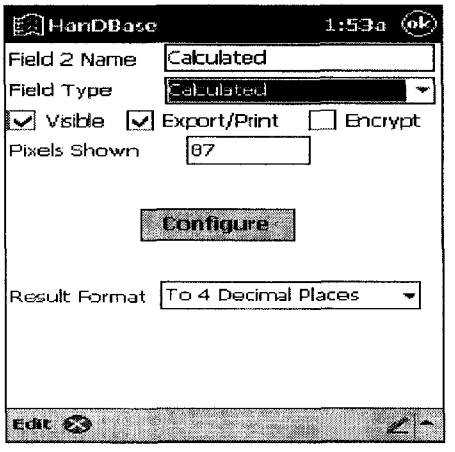


These are similar to a Text field, except the popup choices come from a field of another database. When you select the popup list for this field by pressing the field name to the left of the field, you will be taken to the other database, where you can choose a record by selecting it. Once selected, you will return to the first database, and this field will be filled with the text value of the field specified below in the second database. When selected, the following options appear:

Visible/Print/Export Record/Encrypt/Pixels Shown/Max Characters/Other Database Name/Other Field Name/Default

(See Application Manual for details)

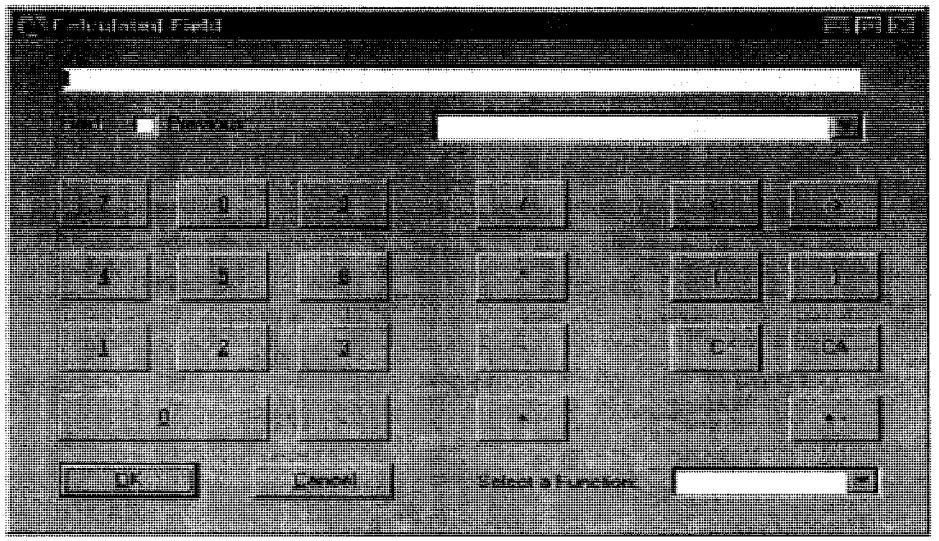
- **Calculated Fields**



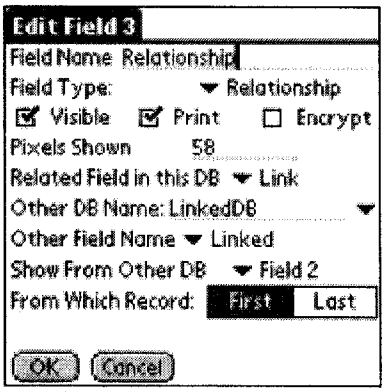
These fields let you perform operations on other fields or constant numbers, operands, using different mathematical functions, operators. The operation can be various combinations of [operand] and [operator], depending on the fields you use and the type of operation you would like to perform on that data. The result of the calculation will be put into this field in the format specified by the Result Format option. When selected, the following options appear:

Visible/Print/Export Record/Encrypt/Configure/Result Format

(See Application Manual for details)



- **Relational Fields**

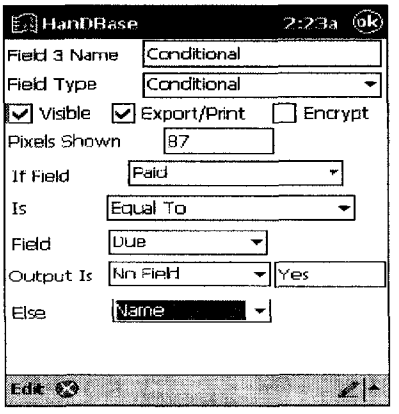


This field enables you to display data from another database within this field, or to link to records in a separate database, based on a specific value in another field of the database. This value can be anything, including text or integers. This field enables much more advanced linking/relationships in HanDBase. You can even establish relationships that display multiple fields from another database that are all based on the relationship you establish.

Visible/Print/Encrypt/Pixels Shown/Related Field in this DB/Other DB Name/Other Field Name/Show from other DB/From Which Record

(See Application Manual for details)

- **Conditional Fields**

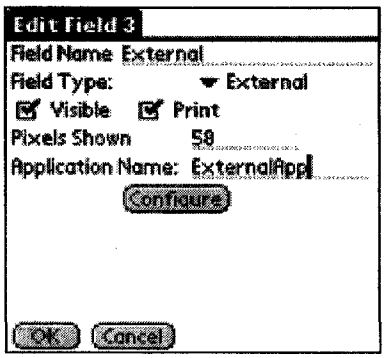


This field allows you to evaluate the values in fields using a conditional statement. This enables a single IF THEN ELSE condition. The result can be a static value or the value from another field. *Visible* Check if you want this field to be visible on the Edit Record screen. Uncheck if you wish to hide it on the Edit Record screen.

Print/Encrypt/If Field/ Pixels Shown/Is/ Field/Output Is/Else Output

(See Application Manual for details)

- **External Fields**



This field allows you to setup plug-ins that you have obtained to add more functionality to HanDBase. These can be things like retrieving data from the Palm Address Book and having it fill in fields in your HanDBase Database, reading a GPS location, dialing a phone number, etc.

Visible/Print/Export Record/Pixels Shown/Application Name/Configure/Encrypt/Other Field Nam&Numbe/Other Database Name&Number/Other Database Name Parameter/Show Value From

(See Application Manual for details)

4.3.2 Data Import & Export

HanDBase Sync Exchange Conduit for Windows is an add-on utility that works with the HanDBase application for handheld device. Sync Exchange enables two unique functions that can be used separately or in combination. You can use Sync Exchange to set up multi-user synchronization to a single HanDBase Database on a desktop computer or server. You can also use Sync Exchange to synchronize your handheld HanDBase database with a Microsoft Access database or ODBC Data Source on a desktop computer or backend server. For example, set up a database that multiple users will synchronize with.

To access HanDBase Sync Exchange for ODBC, you will need to launch the Palm Desktop software. Once opened, you will need to select Custom from the HotSync Menu. This will open the Custom screen. Here you will see a HanDBase 3.0 Conduit listed. Click to Highlight this and then click the Change button. This will open the HanDBase Conduit Settings screen. On this screen, you will see a Sync Exchange button. The functions behind this button enable multi-user synchronization between multiple handheld users, palms, or pocket PCs, to a single desktop database, as well as synchronization with an ODBC database table, also among multiple users, palms or pocket PCs.

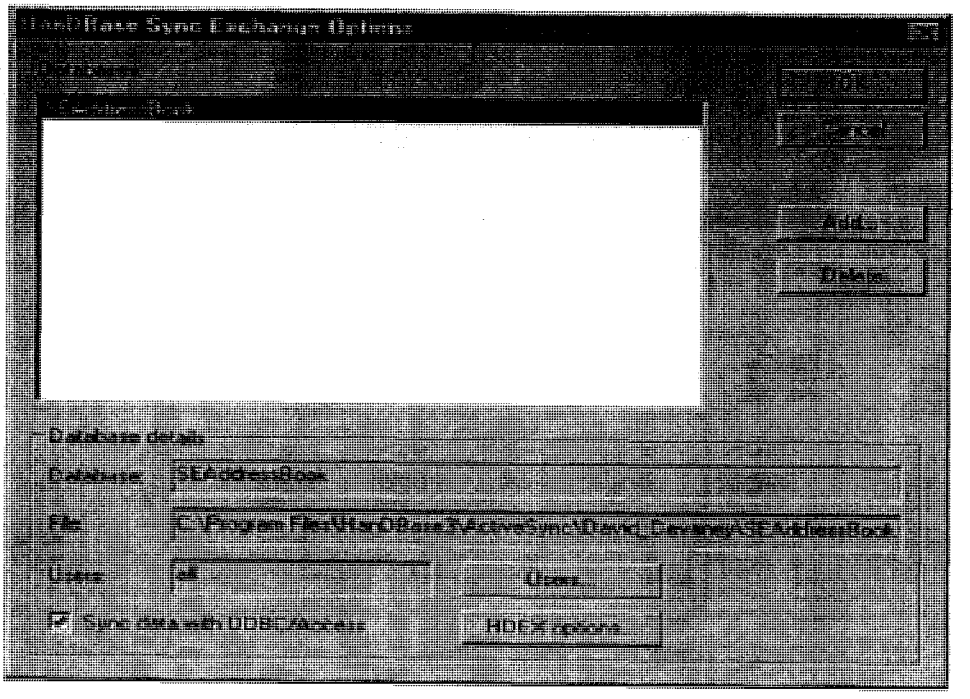


Figure 22: HanDBase Sync Exchange Options

This screen is the starting point for setting up databases to synchronize with multiple users through the HanDBase conduit. This makes it possible to set up a master database on the computer, or even a server, and then have multiple handheld users, palms, or pocket PCs synchronize with that database. That is the basic functionality of this tool. However, this software adds an even more advanced feature. This screen is also the starting point for setting up databases to synchronize directly with an ODBC or MS Access table. Once configured properly, any changes you make on your handheld or in the selected table in the ODBC data source or in MS Access will be synchronized. You can even combine these two options to make it possible to synchronize multiple handheld users with a single ODBC or MS Access database table. When you click the Sync Exchange button, you will see the screen pictured to the left. On this screen are a number of options. Following

is a list of these options and what functions they perform.

This database list shows the databases that are currently set up to synchronize with multiple users or with ODBC. You will see this same list, regardless of which user you access this screen from, as it is universal among all handheld users.

OK Button/Cancel Button/Add Button/Delete Button/Database/File/Users/Sync Data with ODBC/Access/DEX Options.../Synchronize Which Users/All Users/Include Only Selected Users/ Exclude Selected Users/ Available Users/ Selected Users/

(See Application Manual for details)

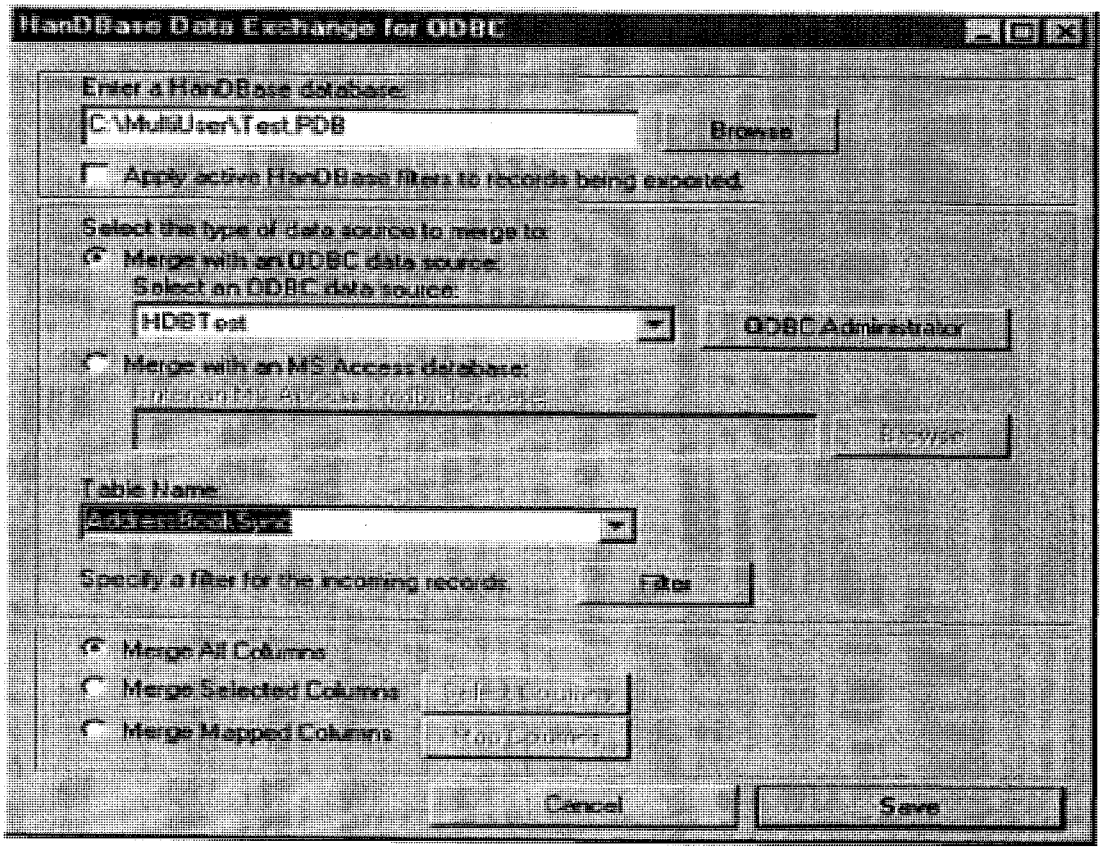


Figure 23: HanDBase Data Exchange ODBC

This screen enables you to configure an ODBC database to synchronize with your HanDBase database. This advanced feature makes it possible to synchronize directly with an ODBC table. This means that, once configured properly, any changes you make in your ODBC data source, including an MS Access database, or in HanDBase will be synchronized or merged together when you synchronize. Following are the options you will be able to set in this screen to enable the synchronization with ODBC.

Enter a HanDBase database

When configuring the synchronization with ODBC, this option will already be filled out, based on the database you chose to synchronize for this option.

Apply active HanDBase filters to records being exported

If you check this option, then ONLY the records that are in the current filter range will be synchronized with the HanDBase database.

Select the type of data source to merge to

This option is only available in the ODBC version of Sync Exchange.

Merge with an ODBC data source

Select this option if you would like to synchronize with an ODBC data source. You can click the ODBC Administrator button to view the existing data sources and to add addi-

tional ones. Use the dropdown selector under Select an ODBC data source to choose which ODBC data source you want to synchronize with.

Select *Merge with an MS Access database* option if you would like to synchronize directly with an MS Access database file. To select an existing MDB file, click the **Browse** button to the right and then navigate to the location where your Access database is. Then select that database and click Open. You can also type in the path to a new Access database file you want to create and then synchronize with it. HanDBase Sync Exchange has the ability to create a new MS Access database from scratch, if you choose that option.

Table Name

Here you can select an existing table you want to synchronize with, if you have selected an ODBC data source or an existing MDB file. Otherwise, you can type in a new name for the table you want to create. Additionally, if you have selected an existing ODBC data source or MDB file, you can still type in a new table name to synchronize with.

Filter

This feature enables you to enter parameters to filter the data you are importing. This feature is designed to be used by users who are familiar with SQL queries and statements. The parameters you will enter are basically what you would enter as part of a WHERE clause in an SQL query or statement. We use the ANSI SQL syntax for these parameters, so you will need to use the same for the portion of the clause you will be entering.

4.4 Pocket PC-Based Database

The interface of pocket PC-based database, similar to Palm-based database layout, offers ambulance staff a familiar way of accessing and indexing patient information and setting properties for each patient record they create. Patient records can also be easily viewed, edited, filtered, sorted, and searched if necessary. Having the feature of open database connectivity (ODBC), patient information on pocket PC can be transferred to or from other ODBC-enabled database applications.

Figure 24 to figure 29 show the pocket PC-based database layout and the process of data input in detail. The ambulance staff opens a database named AmbulanceCallReport presented in Figure 24. Figure 25 exhibits the patient personal information synchronized from the EMS database. The ambulance staff can get the name of the patient, mailing address. Figure 26 displays the hospital registration number, date of birth, and health card number of the patient. The ambulance staff inputs the pickup location, pickup location code, and sending hospital shown in Figure 27. In Figure 28, the record is sent to the designated net printer in the hospital where the patient will be sent. Successful sending records will be saved on pocket PC listed in Figure 29.

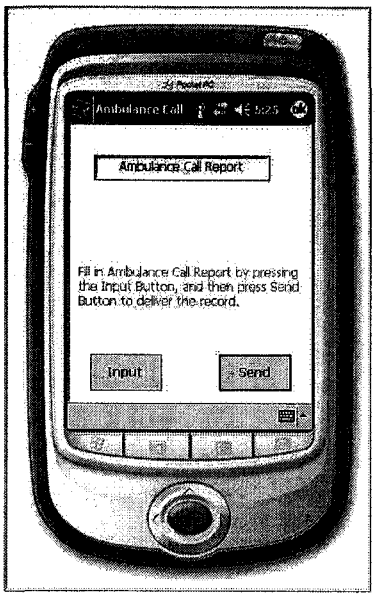


Figure 24: Pocket PC 1

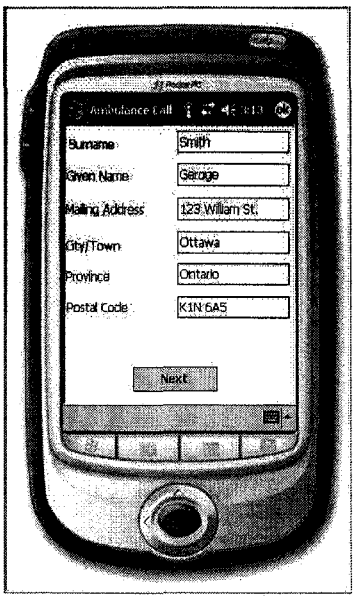


Figure 25: Pocket PC 2

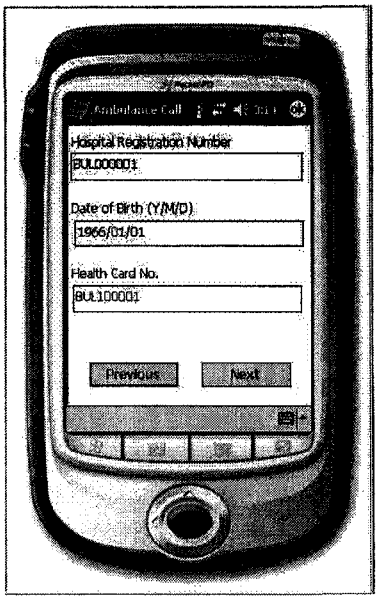


Figure 26: Pocket PC 3

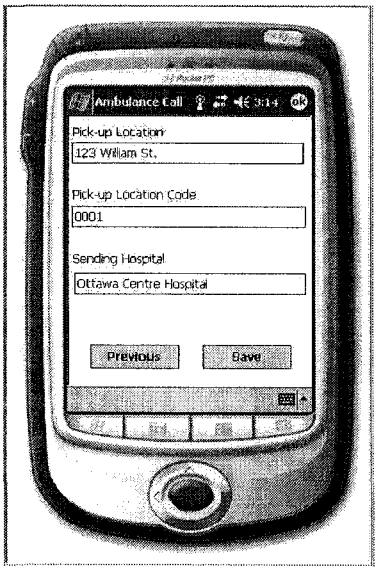


Figure 27: Pocket PC 4

Figure 28: Pocket PC 5

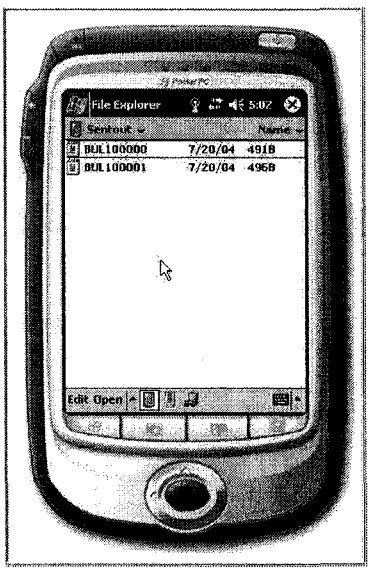


Figure 29: Pocket PC 6

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORK

CONCLUSIONS

This thesis presents the design, implementation, and measurements of handheld Wi-Fi applications in the ambulance systems. The design and implementation in this thesis focus on the information that is transferred from the ambulance fleet to the hospital using Wi-Fi technology for an experimental prototype. In setting out to create the advanced ambulance systems, the main design considerations are mobility and efficiency.

5.1 Mobility

The handheld Wi-Fi applications in the ambulance systems presents a solution that allows the ambulance staff to access remote resources in EMS from any location and record life measurements on site by using handheld PCs, as well as transfer patients' life measurements to the ER on the way to the hospital.

Since patients' life measurements are received before the ambulance reaches the hospital, the handheld Wi-Fi applications provide instant information transportation support for both ambulance staff and healthcare staff. The handheld Wi-Fi applications provide ambulance staff with more flexibility and high performance in accessing and sharing pa-

tients' life data between the ambulance centre and hospitals in time-sensitive circumstances.

5.2 Efficiency

Wi-Fi technology provides time-saving innovations. Handheld PCs are configured to allow EMS personnel to record critical patient information and basic health status variables in the field and transfer such information to the ER prior to or upon the patient's arrival. This data will be particularly useful in enhancing emergency care for crash and accident victims.

A customized software application is installed in handheld computing devices, which allows the user to easily and quickly input the patient's information and health status through a touch-sensitive screen. Data collected on the handheld devices can be transferred to the emergency room through a wireless transmission named Wi-Fi and converted to a standard form. The output can also be printed at a WLAN-enabled printer in the ER. Data collected on the handheld units can be uploaded to a desktop PC at the end of each work shift. Allowing EMS personnel to enter patient data during or between calls has been shown to increase the accuracy of the data collected, reduce the total time required to complete mandatory reports, and improve the timeliness of report submission.

FUTURE WORK

The limitations of current work on the design and implementation of the handheld Wi-Fi applications in the ambulance systems should be seen as avenues for further research. Even though a wireless LAN offers many benefits, hospitals need to consider potential issues before diving into deployment. The following are some items to consider.

5.3 Potential Security Threats

The 802.11 security mechanism, wired equivalent privacy (WEP), does not provide much protection, because a hacker using common tools available from the Internet can decode WEP-encrypted data with enough patience. Hospitals must deploy additional security mechanisms such as SSL-VPN to protect sensitive information.

5.4 Performance Issues

The use of wireless LAN in a hospital requires bandwidth. For example, there could be a hundred devices actively accessing network resources at the same time. This can easily bog down a local access point. In order to accommodate a high density of users, hospitals should consider the use of an ***802.11n*** network to maximize capacity, which is capable of up to 248Mbps throughput.

Future efforts will address how to increase the frequency of data transfer from the field into the ER as a priority. Additional investigation will further examine the information

privacy and security issues pertaining to patient information and its transfer via such systems.

REFERENCE

1. Lassey M., Lassey W., Jinks M., *Health Care Systems around the World*: Characteristics, Issue, Reforms, Prentice Hall, 1997
2. Office of Health and the Information Highway, Policy and Consultation Branch, Health Canada, *Tele-homecare: An Overview Background Paper for Discussion*, May 1998
3. Kun L. G., *Telecommunications and the Reform Process in Public Health*: A presentation at the Health Ministers' Forum, Health Telecom'97 and Infomedica '97.
4. Dan Cwenar, Access Data Corp., *Making Wireless Work for You*: Hype aside, wireless technology can make your business more efficient – if it's used wisely, 2001
5. *The Next Generation of Electronic Health Records*: Vol. 13, No. 25, Committed to Enhancing the Health Information Profession, December 10, 2001
6. Gratzer, D. *Better Medicine, Reforming Canadian Health Care,* 2002, ECW Press, Ontario
7. Lewis, S. et al. *The future of Health Care in Canada.* BMJ; 323; October 2001
8. Klatt, I., *Understanding the Canadian Health Care System.* Online: http://data.cfpboard.org/downloads/abract01.pdf
9. Pollard, S., *Canadian Health Care*, Report commissioned by Civitas, 2002
10. Jonathan Knudsen, *Wireless Java: Developing with J2ME*, 2nd Edition, 2003
11. Lonnon R. Foster, *Palm OS: Palm Programming Bible*, IDG Books Worldwide, Inc.
12. Neil Rhodes & Julie McKeehan, *Palm Programming: The Developer's Guide*, O'Reilly and Associates, Inc. 1999

13. Greg Winton, *Palm OS Network Programming*, O'Reilly and Associates, Inc., 2001

14. Eric Giguère, *Palm Database Programming: The Complete Developer's Guide*, John Wiley & Sons, 1999

15. C. Enrique Ortiz, Eric Giguère, *Mobile Information Device Profile for Java 2 Micro Edition (J2ME): Professional Developer's Guide*, John Wiley & Sons, 2001

16. Related Web Sites: http://www.palmopensource.com/index.php3?category=26
http://www.palmos.com/dev/support/docs/

17. Frank Quick, *Security in CDMA Wireless Systems*, Qualcomm Inc., February 1997

18. Mullaguru Naidu, *Security Aspects of Mobile Wireless Networks*, July 2002.

19. Microsoft, *An Introduction to the Windows 2000 Public-Key Infrastructure*, http://www.microsoft.com/technet/archive/windows2000serv/evaluate/featfunc/pkiintro.mspx

20. *Digital Signature Guidelines Tutorial* http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

21. Netscape Communications, *The SSL Protocol*, Version 3.0, 1996

22. Andrew Nash, William Duane, Celia Joseph and Derek Brink, *PKI – Implementing and Managing E-security*, Osborne/McGraw-Hill, 2001.

23. RSA Security, *PKCS #11: Cryptographic Token Interface Standard v2.2*, 2004

24. Joseph Steinberg, *Understanding SSL VPN,* March 2005

25. Elaine Smyth, Kevin Curran, *Wi-Fi Security*, Sept. 2004

26. Matthew Gast, *802.11 Wireless Networks*, April 2005

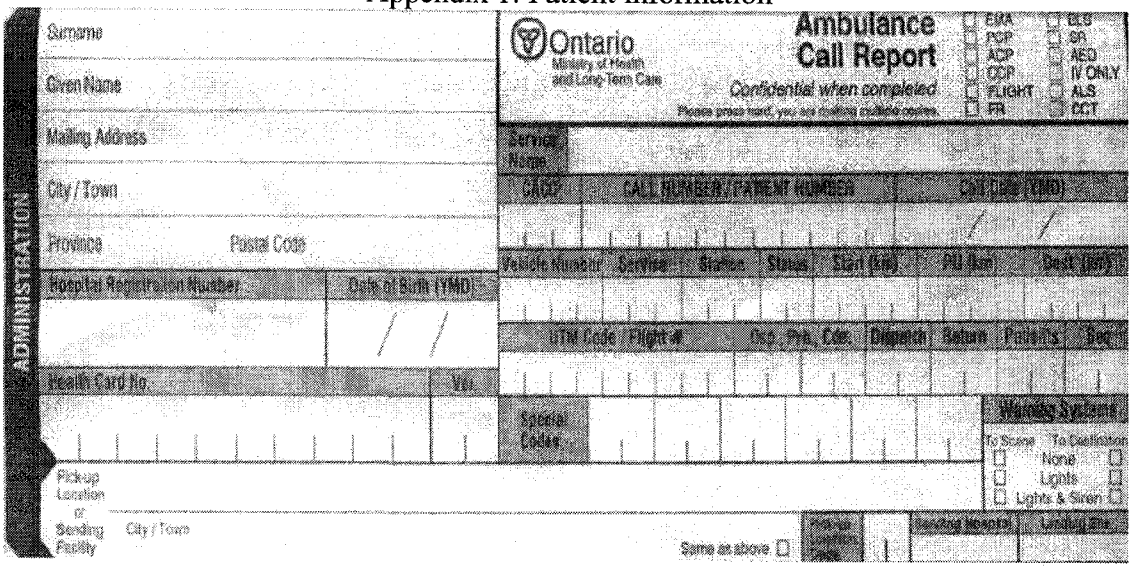
27. Weidong Kou, *Networking Security and Standards*, 1997

28. Dobromir Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*, June 2007

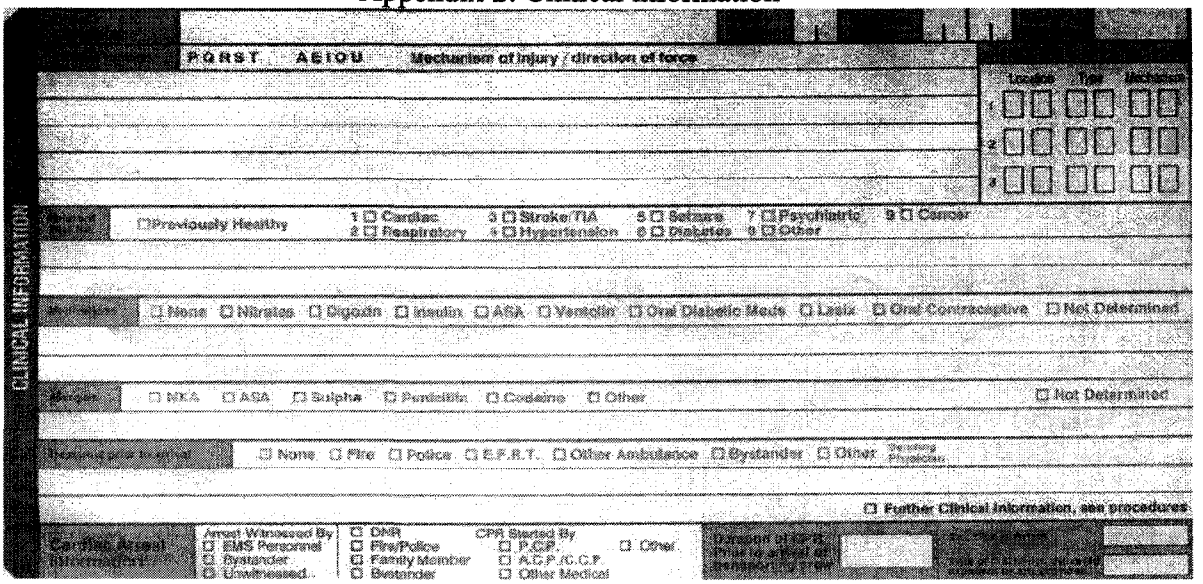
APPENDIX

Ambulance Call Report Developed by the Ministry of Health and Long Term Care

Appendix 1: Patient information



Appendix 2: Clinical information



Appendix 3: Physical exam