Department of Electronic and Electrical Engineering

Loughborough University

A HIGH-SPEED WIRELESS NETWORK USED FOR TELEMEDICINE

Zhicong LU BSc

A thesis submitted in partial fulfilment of the requirements for the award of Master of Philosophy at Loughborough University

November 2005

Supervisor: Professor Bryan Woodward DSc, PhD, DIC, CEng, FIEE, FIOA, FRGS

Underwater Acoustics Research Group

Department of Electronic and Electrical Engineering

ABSTRACT

Nowadays, there is growing interest in using telemedicine to provide non-face-to-face healthcare for patients. The emergence and development of WLAN (Wireless Local Area Network) technology, which supports high-speed wireless communications within the existing Intranet that covers the healthcare system, makes it possible to provide routine body check-ups for patients who need long-term monitoring.

In this thesis, we present the design of a wireless telemedicine system using WLAN technology. The system features low cost, easy set-up, reliability and future improvability. Mobile patients are periodically sampled for medical data, which are sent to the hospital server for storage and display via the WLAN, so that a healthcare group can routinely monitor the patient "on-line". The thesis describes details of the conceptual hardware design for a mobile patient module, which comprises a control module and application modules. It also supports software upgrades simply by linking the control module to a personal computer. In the software design, the thesis highlights the database manipulation, server implementation and user interface design. We form a specific data packet format to standardise the data interpretation, perform user authorisation to maintain information security, and design user-friendly interfaces to avoid any difficulty in operation. To enhance security for patients' records and for monitoring efficiency and data reliability, we present a data handling method that contains both encryption and compression.

ACKNOWLEDGEMENTS

I would like to express my gratitude and appreciation to my supervisor, Prof. Bryan Woodward, for his precious advice and valuable instruction in the process of my research. Under his direction, I started with a thorough understanding of my research area. I have great respect for his attention and time.

A special note of thanks should be recorded for my colleague, Dr Fadlee Rasid. In our discussions, he had provided valuable information and help, so that I could go deep into my research and accomplish much more.

I would like to extend my thanks to the staff of the Department of Electronic and Electrical Engineering for their assistance in my research, and to the staff of the Pilkington Library of Loughborough University for their help in searching for useful information.

I would to add my grateful thanks to my parents and elder brother for their support throughout the years.

Also, I should like to acknowledge the support of all my friends.

FIGURES

TABLES

CONTENTS

CHAPTER I

INTRODUCTION

"The world is a fine place and worth fighting for."

—— *"For Whom The Bell Tolls"*
by Ernest Hemingway

1.1 Telemedicine

In recent years there has been a massive increase in chronic diseases worldwide. Since 2004, heart disease has become one of the main killers in the world [1]. Statistics from the American Heart Association show that one out of every five Americans has some kind of heart disease, yet the number is still rising at an alarming rate [2]. In 1985, around 30 million people in the world had Type 2 diabetes. But today, in Europe alone, 48 million people are living with this disease, which is 7.8% of the population; India has 35.5 million cases; China has 23.8 million and the U.S. has 16 million [3]. Hence, there is an acute need for more technological advances to be used in the management of these chronic conditions.

Patients with chronic diseases require routine healthcare, and telemedicine might be a good solution. Telemedicine can be considered to be the delivery of healthcare and the sharing of medical knowledge over a distance, with the help of information and remote communications technology [4-7]. Equipped with reliable telemedicine equipment, patients living in rural or remote places can be "monitored" on-line in real time. This equipment samples the patient's body-status data and sends these data to a hospital, clinic or surgery, so that doctors can evaluate the patient's health periodically [4, 8]. As a result, patients can enjoy home-healthcare, following their doctor's instructions. In this way, we can regard telemedicine as the complement or extension of a traditional healthcare service.

The concept of telemedicine was first introduced thirty years ago. Compared with traditional face-to-face healthcare services, it benefited by allowing remote-medical consultations, so that a patient could exploit telecommunication networks, and therefore overcome the problem of being distant from a hospital. It also shortened the time involved in attending to patients, especially for medical emergencies, and freeing hospitals from the overload problems [7, 8]. On the other hand, a telemedicine system provides medical information sharing, enabling co-operation among doctors and specialists in different areas from other hospitals, which considerably improves the quality of medical services [7, 9, 10].

Originally, telemedicine systems were built using hard-wired communications systems, such as Public Switched Telephone Network (PSTN), Plain Old Telephone Systems (POTS) and Integrated Services Digital Network (ISDN) [7]. Some of the mature areas of telemedicine include teleradiology, telecardiology and telepathology [4, 10-16].

A further bonus of telemedicine has been to achieve mobility, which was impossible with traditional systems, by employing mobile technologies, especially the deployment of second generation (2G) mobile cellular networks, such as the Global System for Mobile Communications (GSM) network, which covers over 95% of the population of the Europe [15]. Satellite communications has also been used for telemedicine, which allows connection, at least theoretically, to anywhere in the world [17, 18]. On the one hand, mobility sets patients free from fixed locations, allowing them to move at high speed over large areas. Some projects provide telemedicine services on board airplanes on long distance flights [19]. Also, it opens up new application areas for telemedicine. An application of the AMBULANCE project using the GSM network has allowed emergency cases to receive effective pre-hospital treatment in moving ambulances following a doctor's instructions [15]. The idea of giving remote patients daily check-ups sounds practical with mobile networks. Portable devices connected to a mobile phone allow patients to carry on their daily routines while being monitored. Other research has concentrated on the application of GPRS (General Packet Radio System), an enhancement of the GSM network that supports an instant and permanent mobile connection [4]. However, the major drawback of these technologies is the limited up-link data rates, and a restriction on the transmission of large amounts of data [4].

New developments of short-range wireless communications technologies allow other telemedicine applications. These technologies are so called "fixed wireless access", which cover only a limited area and need fixed gateways linking to hard-wired networks for long-distance transmission. A Bluetooth PAN (Personal Area Network) can set up a wireless coverage for all biosensors that are placed on any part of the skin surface of the human body, allowing free patient movement with whole body monitoring [4]. A home-RF system features an easy set-up and reliability. Any implementation requires a portable device embedded with an RF transceiver to transmit ECG and blood pressure signals cordlessly to a fixed unit, which then transmits the signals to the hospital via PSTN [13]. Some applications use the technology of the Wireless Local Area Network (WLAN) with a Personal Digital Assistant (PDA) [4, 8, 20]. Some implementations of Medical Wireless LAN (MedLAN) provide healthcare for accidents and emergencies within hospitals covered by WLAN [21]. These technologies provide high data rate transmission; however, the limitation is that only low speed movement within a limited coverage area is allowed.

One solution to the problem associated with mobile cellular networks and short-range communications is the third generation (3G) technologies, which provide high enough data rates for both high-speed movement and office use within wide coverage. Some researches on 3G-telemedicine systems are now under way [4, 17, 22, 23]. As a combination of telecommunication technologies and medical care, telemedicine keeps progressing, allowing more and better healthcare services to become available.

1.2 Objectives of the Thesis

This thesis presents the design of a mobile telemedicine system based on WLAN technology. It focuses on an outline of the system architecture, details of the hardware (mobile patient unit) design, software implementation, and the data handling for security and efficiency before medical data transmission.

A literature review in Chapter II discusses the development of telemedicine and the current state of the art. It suggests a definition and classification for telemedicine, stresses the importance of wireless telemedicine, and discusses the basic principles of WLAN technology. The applications and potential of telemedicine have gained interest as a research topic, with plenty of scope for improvement.

In Chapter III , we present the design of a wireless telemedicine system using WLAN technology. The system features easy set-up, reliability and future improvability. It allows mobile patients to be monitored within the coverage area of the WLAN in the hospital, by transmitting their medical signals to a hospital server with a database, which can be accessed "on line" by a local healthcare group or by doctors who are away from the hospital.

The first section of Chapter IV describes the modular hardware design, which comprises a fixed control module and a changeable application module. The control module contains a WLAN transceiver and a central micro-controller system. It receives data from an application module, stores or processes the data, and in most cases sends the data to the hospital server. An application module differs in its functionality, such as data sampling and hardware system upgrade. This structure makes it adaptable for a variety of applications. The hardware system also features "improvability".

The second section of Chapter IV describes the software design of the system. We present the implementation of the MySQL database, a database server, the client software for doctors, and a software simulation of the mobile patient unit.

1) We design a tailored database for the mobile telemedicine system. It contains personal information and medical data for each patient.

2) We have also produced a multi-client server for database access. It communicates with patients via a Local Interface (LI) and with doctors via a Remote Interface (RI). The LI interprets data from patients and updates their medical records. The RI is a doctor browser installed in doctors' devices, allowing authorised doctors to read and change data in the database.

The third section of Chapter IV presents a data handling method using a particular data packet format for security and efficiency during transmission. To maintain patient confidentiality in the open wireless environment, we apply both encryption and compression. We use the 64-bit key (56 bits in use) DES (Data Encryption Standard) algorithm to encrypt the patient data before transmission. To cut down the transmission time, the data are compressed using the Huffman algorithm, which can reduce the data size without any information loss, i.e. lossless compression.

Finally, Chapter V summarises the thesis and draws a conclusion, as well as suggesting further improvements and potential future research themes for advancing telemedicine.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction to Telemedicine

2.1.1 Definition

The concept of telemedicine was first introduced around thirty years ago. It can be defined as "medicine at a distance", i.e. the provision of healthcare and the sharing of medical knowledge over a distance, using information and telecommunications technology [4-7].

At the current stage, a new concept of "m-Health" has emerged. M-Health can be defined as "mobile computing, medical sensor, and communications technologies for healthcare" [4]. To facilitate healthcare, it utilises mobile communications technology for medical diagnosis, treatment, and patient care [16]. An efficient m-Health system enables a physician or specialist at one site to handle the full means of healthcare to remote patients, including diagnosing patients, giving intra-operative assistance, providing therapy, or consulting with another physician or paramedic at another remote site [6]. Further, allowing healthcare to be administered outside a hospital setting is seen as an important way of reducing medical costs [8, 24]. Thus, currently m-Health is a significant area of research and development.

As a new area of the healthcare, m-Health aims to provide expert-based healthcare to under-staffed remote sites and to provide advanced emergency care [6]. A patient from a rural area could be given a routine check without having to commute to a hospital on a regular basis. Routine inspections and monitoring can be done while the patient is at home or at work, or even on the move, thus relieving resources for more demanding cases in hospitals [8]. In this case, choosing a proper communication technology should be taken into consideration carefully. A well-applied technology can improve efficiency and effectiveness, which means lower costs, less time wasting, and increasing direct attention to patients.

2.1.2 Evolution

The evolution of telemedicine tends to keep in step with the development of telecommunication technologies. Traditional telemedicine systems were based on fixed wire communications. Some designs and implementations using the public switched telephone network (PSTN) and integrated serviced digital network (ISDN) have been introduced in other papers [7]. Over these wide area networks, the medical information from a remote patient could reach the hospital at a doctor's request. The main drawback of these systems is the patient's limited mobility. Thus, they are in fixed locations, which has somewhat restrained the deployment of telemedicine.

In recent years, as the development of modern wireless telecommunication technology, such as the global system for mobile communications (GSM), general packet radio system (GPRS), and satellite communications, we find the solution for the mobility problem by extending telemedicine to a wireless area, which not only greatly frees patients from being forced to stay in a fixed location, but also makes the telemedicine easy to set-up [7, 8, 15, 25]. However, compared with wired systems, the lower data-transfer rates confines the functionality of current telemedicine applications [4].

There has been an evolution of mobile telecommunication systems from the second-generation (2G) to the third-generation (3G), such as the Wideband Code-Division Multiple Access (W-CDMA), as well as the development of the wireless Internet technology, such as the WLAN. All these technologies provide faster data rates, so that some of the telemedicine services requiring high data rates would be implemented wirelessly, while these services are only feasible on wired communication networks at the moment.

Besides the technology aspect, telemedicine has also developed in categorisations. Nowadays, considering the biomedical signals, telemedicine is referred to as telecardiology, teleradiology, telepathology, teledermatology, teleophtlalmology, teleoncology and telepsychiatry, which enables long-term remote monitoring for chronic diseases [7]. In terms of functional aspects, it can be divided into telediagnosis, teleconsultation, teleconferencing and tele-education, allowing communications between patients and doctors in different situations [9]. In a word, telemedicine is able to provide great coverage of healthcare.

2.1.3 Drawbacks

Compared with the traditional "in-patient" scenario, one of the main drawbacks of telemedicine is the poorer interaction between a patient and a doctor. Their relationship is cold: the patient faces silent devices, unable to talk about his feelings, and the doctor reads a set of boring records, without seeing any symptom from the patient, nor giving them any immediate suggestion.

Another drawback is the possible data quality deterioration. In hospitals, the powerful equipment can provide high quality results for precise diagnosis. However, most of the equipment is expensive, bulky, and some of them require professional users, whereas the devices specifically designed for remote patients are affordable, portable, and manageable by general users, which inevitably lead to lower data quality. Besides, higher data quality means larger record size. In the situation of low transmission rate between the patient and the doctor, it is advisable to reduce the data quality for effective reception for the doctor, especially in emergency.

Finally, as a new concept of healthcare, telemedicine might lead to organisational changes. Hospital might set up specialised departments, and doctors might have new working styles as fewer patients go to hospital.

2.1.4 Barriers

Technological barriers are a significant reason why telemedicine might not be adopted. The inadequate capabilities of current technologies seem difficult to fulfil the clinical needs, which include [26]:

1) Sufficient data quality to meet the clinical needs of the healthcare professionals.
2) Sufficiency of real-time continuous motion images.
3) Ability of healthcare professionals to handle the equipment.
4) End-user training and proper use of the telemedicine equipment.

There are other technological demands for a realisable telemedicine system, such as system reliability, ease of use, and concerns about patient privacy and confidentiality using an electronic medium. Patient mobility, one of the features of modern telemedicine, requires support from new technologies.

Cost often becomes another barrier to implementing telemedicine [6]. New equipment is introduced and user training is necessary, since new healthcare styles are adopted for both doctors and patients. Charges for transmission of medical records limit some services from long-term execution.

2.2 Wireless Telemedicine

In the past decades, both wireless telecommunication technologies and their relevant telemedicine systems were developed rapidly. In this session, we briefly describe the main features of some wireless technologies, including the 2G and 3G networks as well as satellite communications, and discuss their advantages and disadvantages, so that to find out whether they are suitable for establishing a telemedicine system or not.

We can divide these technologies into three categories: (a) the mobile cellular networks, including GSM, GPRS, EDGE, and the forthcoming Universal Mobile Telecommunications System (UMTS) and 3G; (b) satellite communications [7]; and (c) short-range wireless networks, like Bluetooth, WLAN and infrared;

2.2.1 Mobile Telemedicine Systems

Mobile Cellular Networks

Table 2.1 list the key features of some mobile cellular networks that are currently in used [7, 27, 28].

	Type	Sub-type	Frequency Band	Data Transfer Rates
2G	GSM	GSM-900/1800/1900	900/1800/1900 MHz	9.6 kbps
2.5G	HSCSD	GSM-900/1800/1900	900/1800/1900 MHz	9.6 – 57.6 kbps
	GPRS	-------------	900/1800/1900 MHz	171.2 kbps
	EDGE	-------------	900/1800/1900 MHz	384 kbps

Table 2. 1 Key features of mobile cellular networks

GSM is a mobile cellular network system that is most widely used. In the standard mode, it provides a data-transfer rate of 9.6 kbps, which does not seem to be fast enough for telemedicine. However, there are three 2.5G upgrades from GSM, namely:

1) HSCSD: high-speed circuit-switched data. Instead of limiting each user to only one specific time slot in the GSM standard, it allows individual users to use up to four consecutive time slots on the GSM network, with each time slot having a data rate up to 14.4 kbps, and therefore a data rate of up to 57.6 kbps overall [27, 29].

2) GPRS: general packet radio system. It is a packet-based data network built on the GSM network, suited for non-real time Internet usage. An individual user is able to achieve up to eight time slots of a GSM radio channel dedicated to GPRS, with a data rate up to 21.4 kbps each, and therefore a data rate of up to 171.2 kbps overall [27, 29].

3) EDGE: enhanced data rates for GSM evolution. It is operated in a new digital modulation format on the GSM network, which greatly enhances the data rate. For a single GSM channel, it supports a data rate about 384 kbps. While combining different channels, it can provide up to several megabits per second of data throughput to an individual user [27, 29].

These upgrades, especially GPRS and EDGE, give higher data-transfer rates, enabling the availability of prompt and accurate medical care. What is more, it takes advantage of the wide coverage of the GSM network, which greatly helps telemedicine deployment.

Some recent studies focus on the real time and non-real time use of the GSM network, and their experimental results, including software simulation, show the feasibility of GSM communications, which are proven to be considerably stable and robust [4, 7, 12, 15].

Satellite Communications Technology

Table 2.2 lists the key features of satellite networks [7, 17, 19]. Satellite systems provide various data rates, ranging from 2.4 kbps to 155 Mbps, so that they can fulfil different medical purposes. Another advantage is that the satellite links are operating theoretically all over the world [7, 17, 18]. Future satellite systems will offer high-speed Internet access and broadband multimedia and IP-based services over IP and/or IP/ATM networks, enabling the home-used satellite services[18]. However, its high cost and professional operating skills for specific equipment keep it out of reach for general and personal use, especially for the purpose of telemedicine that requires many personal communication devices. Instead we aim to design an easy-handling device for both patients and doctors/specialists. Therefore, it dose not seem appropriate to adopt the idea of using satellite communications for common-use telemedicine.

Type	Sub-type	Frequency Band	Data Transfer Rates
Satellite	ICO	C, S band	2.4 kbps
	Globalstar	L, S, C band	7.2 kbps
	Iridium	L, Ka band	2.4 kbps
	Cyberstar	Ku, Ka band	400 kbps – 30 Mbps
	Celestri	Ka band and 40-50GHz	155 Mbps
	Teledesic	Ka band	16 kbps – 64 Mbps
	Skybridge	Ku band	16 kbps – 2 Mbps

Table 2. 2 Key features of satellite systems

2.2.2 Short-Range Wireless Telemedicine

Table 2.3 lists the key features of short-range wireless networks [7, 30, 31].

Type	Sub-type	Frequency Band	Data Transfer Rates
WPAN	Bluetooth	2.4 GHz	723.2 kbps
WLAN	IEEE 802.11a	5.2 GHz	54 Mbps
	IEEE 802.11b	2.4 GHz	11 Mbps
	IEEE 802.11g	2.4 GHz	54 Mbps
	IrDA (Infrared Data Association)	Infrared Light Spectrum	4 Mbps
	HiperLan1	5 GHz	20 Mbps
	HiperLan2	5 GHz	54 Mbps

Table 2. 3 Key features of short-range wireless networks

WPAN

The WPAN (Wireless Personal Area Network) is defined with IEEE standard 802.15. In practice, Bluetooth is one of the most relevant enabling technologies for a WPAN in a telemedicine system. In some researches, a Bluetooth WPAN is established to collect medical signals from different parts of the patient's body, and a central control unit sends the signals to a hospital site by some certain wireless methods, freeing the patient from the restriction of uncomfortable wires [4]. Bluetooth is an open standard providing an ad-hoc approach for enabling various devices to communicate with one another within a theoretical 10-100 metres range. It benefits from a high data rate and the operating power, which makes it easy to be embedded into any portable devices, resulting in great mobility [4]. However, the short range, the connection stability, and the compatibility with different operating systems prevent its deployment in telemedicine.

Wireless LAN

WLAN is a flexible data-communications system, used as an extension or as a replacement of the traditional wired LAN [7, 27]. It is a kind of "fixed wireless access". There is a fixed access point (AP) in the WLAN functioning in two ways: (1) it functions as the adapter between the wireless and wired network, while each mobile unit within the WLAN links to an outer network via the AP; and (2) it functions as a hub in the WLAN for each mobile unit [30]. However, these mobile units can also link to each other directly within a shorter range. A typical wireless coverage ranges from 30 to 50 metres indoor and 100-500 outdoor, depending on the data rate we set. The higher data rate, the shorter is the range. Its high data rate supports the case of large sums of medical signals [4, 30]. Its major drawbacks include the low-speed patient mobility and that the patients are bound in the fixed access point coverage.

At the moment, only a few powerful public access points are located in limited spots all over the world, which leads to little availability of WLAN. To solve this problem, in many studies, a WLAN is built to cover a whole hospital area or a campus, letting the monitored subjects move within this area [20, 31]. The personal access points are also introduced. They can build up a WLAN in a personal site and extend the telemedicine system to the site, but only limited authorised users are permitted.

Fortunately, in the future, the WLAN would become the complement of the WCDMA in hot spots. That means the base station of mobile cellular networks would be compatible to the WLAN, freeing the patients from the fixed separate Access Points (AP) [27]. However, it would face the problem of roaming between the coverage of different APs [32].

Another problem is to build a function platform, meaning a hardware environment, for WLAN, allowing the patient devices to function correctly with the wireless protocol. In several projects, the powerful Personal Digital Assistants (PDA) with embedded or plug-in WLAN devices are demonstrated, which simplifies the design of the patient-unit and grants the patients great mobility, but results in the additional cost of the expensive PDA [4, 20].

Another drawback of WLAN is the low mobility at the maximum speed, around 5 kph, i.e. pedestrian speed, whereas the 3G technologies with lower data rate can support very high speed mobility, as shown in **Figure 2.1** [33].

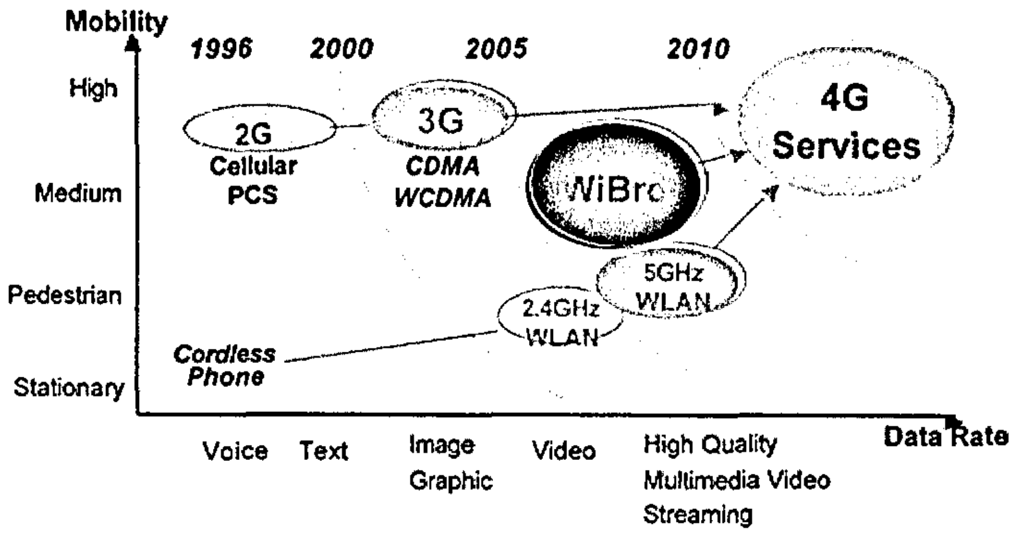


Figure 2. 1 Two system compositions of WLAN

As a result, the features of "fixed wireless access" and low mobility constrain WLAN as suitable only for the telemedicine scenario of all patients moving slowly in an area covered by WLAN, such as a hospital or a primary care centre, and not allowed outside that area.

2.3 WLAN Technology

WLAN was first introduced in 1987 by the IEEE (Institute of Electrical and Electronic Engineers) 802.11 WLAN Working Group. It is designed as the extension or replacement of the traditional hard-wired local area network (LAN) within homes, buildings, and office settings, freeing users from messy cable connections and complicated interface installation [27]. At present, the IEEE has developed an open standard for two-way wireless communications, the IEEE 802.11 protocol, defining that the WLAN operates in the unlicensed 2.4GHz and 5.2GHz bands, and giving it some benefits such as low-power level, low-cost and high compatibility [31].

The WLAN can be installed significantly faster and cheaper than traditional telemetry systems, allowing unprecedented flexibility and responsiveness to organisational needs and changes [30]. Some telemedicine researches and applications have revealed the potential of using WLAN in telemedicine systems within hospital/surgery areas [4, 20, 31]. These systems support a large capacity of medical data and voice services in both point-to-point and point-to-multipoint links, significantly increasing healthcare efficiency. On the other hand, new WLAN products are designed to be smaller in size with universal interfaces, making the portable WLAN telemedicine module possible.

In this section, we provide a brief overview of the WLAN technology principle, including the system structures, function modes and protocols architecture, as well as some key features that are essential to our design.

2.3.1 System Structures

Similar to the hard-wired LAN, there are two different system structures in the WLAN, namely the peer-to-peer structure (ad-hoc mode) and the master-slave structure (infrastructure mode), as shown in **Figure 2.2** [30].

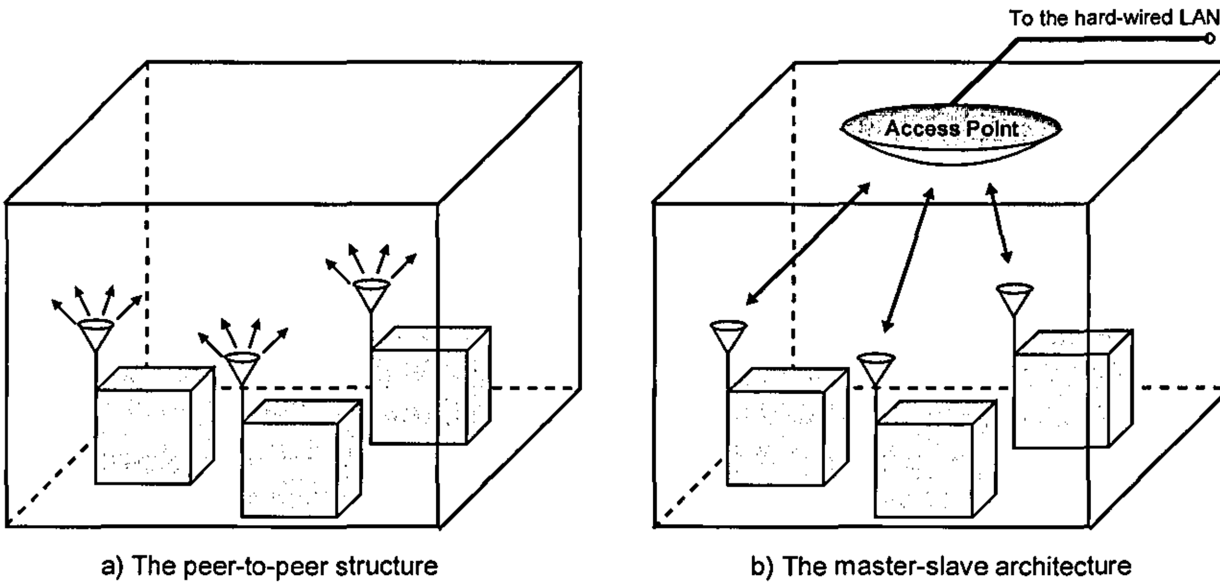


Figure 2. 2 Two system compositions of WLAN

A peer-to-peer structure builds a WLAN that is isolated from the outer network. Each unit in this structure is equal to the others. It has a WLAN transceiver and could only access the units within its range. An AP can also be included in this structure, but it only works as a relay station to extend the WLAN range in this case.

A master-slave structure builds a WLAN that links to the wired LAN via an access point (AP). An AP is a MAC-layer bridge that could be considered as a wireless hub, or an adapter between the WLAN and the hard-wired LAN. Devices in the network can connect to or associate with the AP, and the AP allows one device at a time to either communicate with another device or to the hard-wired LAN.

2.3.2 Specification and Function Mode

There is an overview of the IEEE 802.11a/b/g WLAN standard shown in **Figure 2.3** [34] and its relevant glossary in **Table 2.4**.

		802.11b @2.4 GHz		802.11g @2.4 GHz		802.11a @5.2 GHz	
Rate, Mbps	Single/Multi Carrier	Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

Figure 2. 3 IEEE 802.11a/b/g WLAN standard

CCK	Complimentary Code Keying
PBCC	Packet Binary Convolutional Code
OFDM	Orthogonal Frequency Multiplexing
CCK-OFDM	Complimentary Code Keying - Orthogonal Frequency Division Multiplexing

Table 2. 4 Glossary of WLAN modulations

As shown in Figure 2.3, IEEE 802.11 standards support different data rates. However, the maximum data rate is only available in the ideal environment of non-interference and very short distances. The expected data rates at varying distance of each standard are shown in **Figure 2.4** [35].

Currently, the most popular IEEE 802.11b utilises the spread spectrum modulation, which "spreads" the RF signal over a range of frequencies, enhancing the ability of the RF communication system to avoid interfering noise and providing security against eavesdropping. The IEEE 802.11 defines two types of spread spectrum modulations, namely Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). FHSS provides data transmission rates at 1 and 2 Mbps, and DSSS has been extended by 802.11b to a much higher data rate including 5.5 and 11 Mbps besides the basic 1 and 2 Mbps [31].

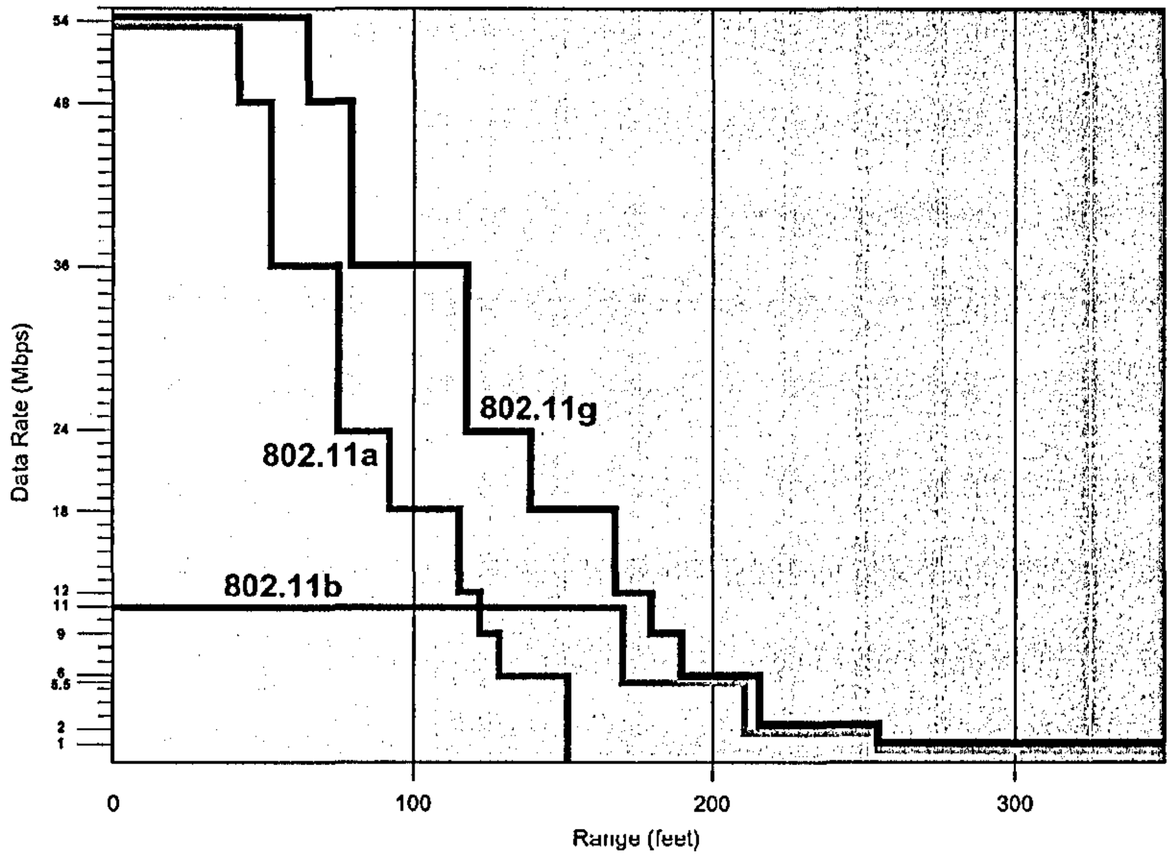


Figure 2. 4 Expected 802.11a/b/g Data Rates at Varying Distance

Frequency Hopping Spread Spectrum

FHSS spreads the spectrum by moving the centre frequency of the broadcast. In decoding FHSS, the receiver must "hop" back from frequency to frequency at the same time as the transmitter.

In modulation, a pseudo-random hopping pattern defines a hopping channel that the carrier frequency of the transmitter hops to, and a hopping sequence dictates the frequency order that the hopping follows. Stations in a cell hop the carrier frequencies at synchronised intervals. The AP transmits synchronisation signals to the mobile units (MU) for time synchroisation. Each hop is at least 6 MHz away from the previous frequency.

In the United States, there are 79 channels and 1 MHz bandwidth each. IEEE 802.11 defines a pseudo-random order of these channels for 802.11 devices to hop through. Besides, up to 15 APs are allowed to be co-located without significant interference problems.

Direct Sequence Spread Spectrum

DSSS keeps the centre frequency of the broadcast constant and uses an Ex-OR spreading function to multiply the signal. Suppose that we have an *n*-bit pseudo-random code. Each bit of the data stream is Ex-OR'd with the pseudo-random code, so that it is spread into the frequency with a bandwidth *n* times of the original one. However, the energy decreases to $1/n$ since it is shared by *n* bits. Thus, the code length *n* is called the spreading ratio or the processing gain, indicating the system noise immunity ability. The higher the processing gain, the more immune the system is to interference. We could increase it by increasing the bandwidth of the transmitted signal or by decreasing the data rate. The FCC requires a minimum processing gain of 10. The receiver recovers the data in the same encoding pattern.

For 1 and 2 Mbps DSSS, the length of the pseudo-random code (Barker code) is 11. IEEE 802.11 specifies 14 overlapping channels in 22-MHz Bandwidth with 5-MHz spacing between centre frequencies. In the United States, channels 1-11 are available, so three channels of 1, 6, and 11 are non-overlapping.

The IEEE 802.11b uses Complementary Code Keying (CCK) that uses an 8-bit code to represent 6 bits of data, so that it achieves a higher data rate with the same 22 MHz channel.

IEEE 802.11a and 802.11g

The standards of WLAN for higher data rate are the IEEE 802.11a operating in 5.2GHz ISM band and 802.11g in 2.4 GHz ISM band. Both of these two standards provide a data transmission rate up to 54 Mbps. 802.11a uses Orthogonal Frequency Multiplexing (OFDM) technology, which is superior to DSSS in term of resistance to multi-path propagation effects, but one can expect shorter range due to the higher frequency and higher data rate. 802.11g uses CCK-OFDM, supporting roaming capabilities and dual-band use for public WLAN networks, while supporting backward compatibility with 802.11b technology.

WLAN Technology for Telemedicine

Due to the short range of IEEE 802.11a, we take the 2.4 GHz WLAN standard into consideration, which mainly focuses on the discussion of the advantages and disadvantages of FHSS and DSSS, the most commonly used technologies.

Compared with DSSS, FHSS has some advantages. FHSS systems are easily co-located, which is quite important for large-scale telemedicine systems. On the other hand, the 6 MHz channel interval and 79-channel capacity frees FHSS from interference and channel blocking, whereas DSSS has only three non-overlapping channels. In other words, FHSS is more reliable[31].

On the other hand, DSSS provides a much higher data transmission rate, approximately 5-10 times to FHSS. However, as mentioned before, this high data rate is only available in the ideal environment of non-interference and very short distances due to the feature of packet fragmentation, which will be discussed later in this section. Thus, we may apply the FHSS and DSSS into two different situations.

The FHSS is competent for the case that we build a WLAN telemedicine system that covers the whole hospital area, which requires the combination of several WLANs that usually work in great load. A hospital can be considered as a noisy environment. It has different purposes, such as different medical data transmission (ECG, EEG, and blood pressure, etc.), voice-conference, and tele-trainings, as well as a huge number of different kinds of users like doctors, patients and specialists. It also has all kinds of medical equipment that might become interference sources. What is more, patients may be moving, which may affect the data transmission. In this case, we have the requirements of easy set-up, reliability and noise immunity, which are the superior features of FHSS to DSSS.

In the house of a rural patient, the situation is different. A single WLAN can provide enough capacity, while the system function is uncomplicated. The home-used devices would not affect the system operation. Patients with chronic diseases are generally advised not to make quick movements, so they only move slowly around the house. The only requirement is the data transmission rate, because in the long-range transmission, shorter transmission time means a lower probability of data errors. In this case, DSSS would be chosen.

2.3.3 Protocol Architecture

In Jun 1997, the original IEEE 802.11 specification was ratified as the wireless extension of the IEEE 802.3, a communications standard for hard-wired LANs that use physical cables and the Ethernet protocol[27]. Therefore, these two protocols are quite similar.

In implementation, the IEEE 802.11 protocol is composed of several layers. Sequential from the lowest layer, they are the physical layer, the link layer, the network layer, the transport layer, and the application layer, among which the first two layers are different from the 802.3 [31]. **Figure 2.5** shows the architecture of these two layers in IEEE 802.11b [36].

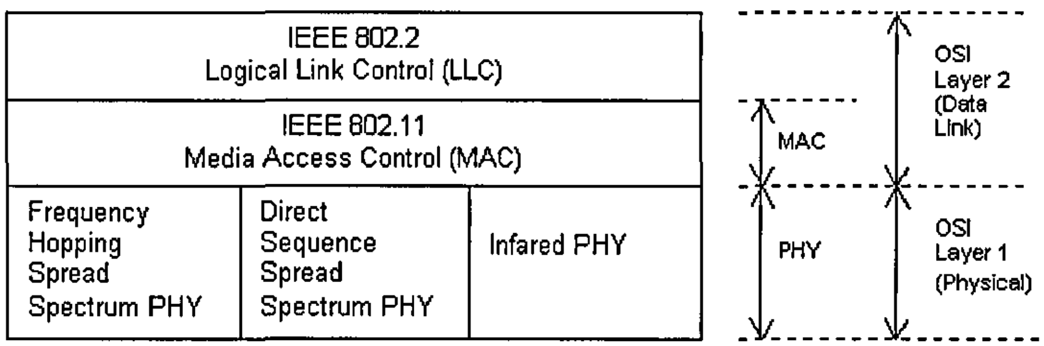


Figure 2. 5 Layer architecture of IEEE 802.11b

The physical layer describes how and how fast the data are transmitted. The IEEE 802.11 defines three physical layers: FHSS in 2.4 GHz band, and DSSS in 2.4 GHz and infrared. Two new physical layers are added in 802.11b to cope with the basic DSSS, supporting data rates up to 5.5 Mbps and 11 Mbps. As mentioned in the DSSS modulation, to gain a better data transmission in the noisy environment, 802.11b uses a dynamic data transfer rate mothed. In a perfect environment, the user may have the maximum 11 Mbps data rate. And the data rate may change dynamically to 1 Mbps, 2 Mbps and 5.5 Mbps when the environment changes [31], for example, for a longer transmission distance, in a different position, or encountering a strong noise. This method ensures the wireless connection is alive, and helps maintaining user operation.

The link layer deals with data transmission status, such as data quantity, transmission failure determination and management, and transmission time. These processes are invisible to users, but they affect the data rate, which is sensible to users [27]. The 802.11 Medial Access Control (MAC) in this layer is quite similar to 802.3. It is designed to avoid data loss in case where the transmission might experience interference. The MAC is the same for all three 802.11 physical lays. The physical and MAC layers cooperate with each other to determine whether the channel is clear or not [31].

Different from the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) in 802.3 MAC, 802.11 uses the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to avoid the "Near/Far" error, which is a typical error in wireless communications [27, 29, 31]. CSMA/CA works by having the sender listen to the channel before attempting a transmission. If the channel is busy, the sender defers the transmission and listens to the channel sometime later. After the transmission, the sender keeps waiting for an ACK (acknowledge) message from the recipient as the signal of successful data receiving. If data are not received or are received with an invalid CRC (Cyclic Redundancy Check), the transmitter will not receive the ACK then automatically retransmits the data after the overtime waiting.

The 802.11 MAC also performs packet fragmentation, which is very useful in large-packet transmission. Large packets are broken into smaller sections to reduce the transmission time for each section, so that the probability of corruption is decreased, especially in very congested environments or noise conditions, and hence, it reduces the needs for re-transmission. The received fragments reassembly is done by the MAC layer in the receiving part, which is transparent to higher-level protocols [31].

The same as the IEEE 802.3, the 802.11 uses IP packets to finish information exchange. An IP packet format is shown in **Figure 2.6** [37].

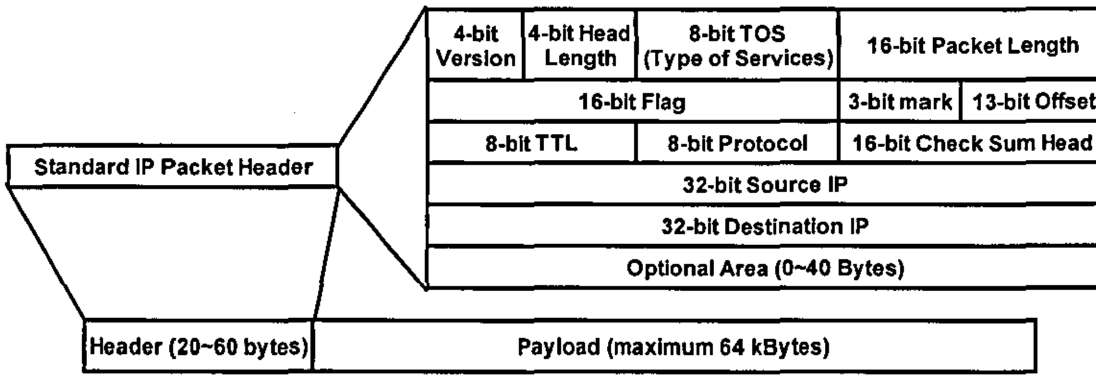


Figure 2. 6 The IP packet format

2.3.4 WLAN Security

The IEEE802.11b standard adopts an optional encryption scheme called Wired Equivalent Privacy (WEP) to secure WLAN data streams [38, 39]. The algorithms of WEP mechanism enable RC4-based, 40-bit key data encryption, providing an equivalent level of security and privacy comparable to a wired Ethernet 802.3 LAN. WEP uses a symmetric scheme in which the same key and algorithm are used for both data encryption and decryption. It benefits from the following two features [39]:

1) Access control, to prevent illegal users without the correct key from access to the network.
2) Privacy, to prevent WLAN traffic being captured by encrypting data streams and allowing decryption only by users with the correct keys.

In WEP encryption, the 40-bit secret key and a 24-bit initialisation vector (IV) are concatenated to form a 64-bit key as the seed of the pseudo-random number generator (PRNG), which generates a pseudo-random key sequence. Then the key sequence encrypts the plain data by doing a bitwise Ex-OR operation, resulting in a data stream with a length equal to the original stream. **Figure 2.7** describes the WEP encryption algorithm.

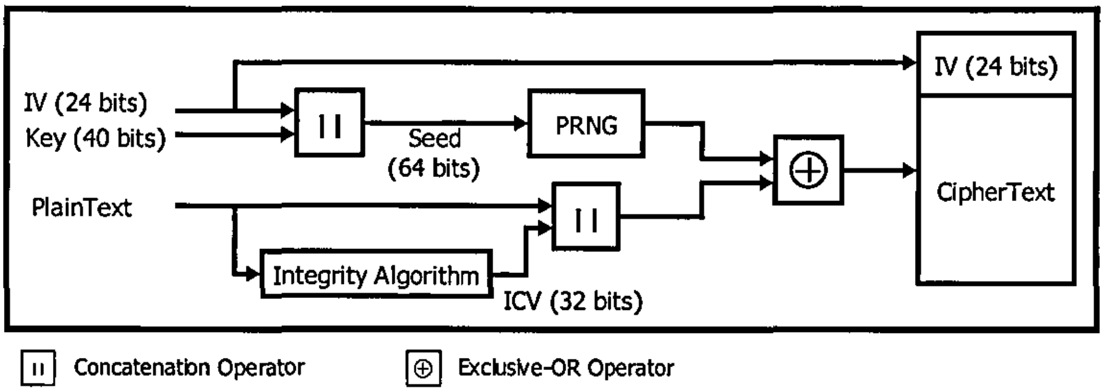


Figure 2. 7 WEP encryption algorithm

However, the data size in transmission is 56 bits (7 bytes) larger, in which the 32-bit integrity check value (ICV) generated by an integrity algorithm (CRC-32) is also encrypted by the key sequence to protect against unauthorised data modification, and the other 24-bit IV is transmitted for decryption at the receiving end.

The one-to-one correspondence between the IV and the output makes the data in high-layer protocols predictable, which reduces the degree of privacy because an eavesdropper can readily determine portions of the key sequence. Thus, the IV is supposed to be changed after each message to preserve the effectiveness of WEP, but that increases the complexity in implementation. Several new products use more secure algorithms, such as the triple data encryption standard (Triple DES) and the elliptic-curve cryptography (ECC), to overcome the drawback of WEP[39], and the later WLAN standard IEEE 802.11i uses the encryption algorithms of both 128-bit key WEP, an enhanced WEP mechanism, and the 128-bit key advanced encryption standard (AES) to increase the data privacy [40]. However, in the aspect of 802.11b, it is required to adopt a security method to provide a higher privacy during data transmission.

CHAPTER III

SYSTEM DESIGN

3.1 System Requirements

A telemedicine system can be simplified into three parts that include a patient record transmitter, a receiver for a doctor in a healthcare system, and a communication channel for data transmission over a distance between the two sites, as shown in **Figure 3.1**. Accordingly, the system requirements can be categorised into these three aspects, throughout which we can define the requirements for the overall system.

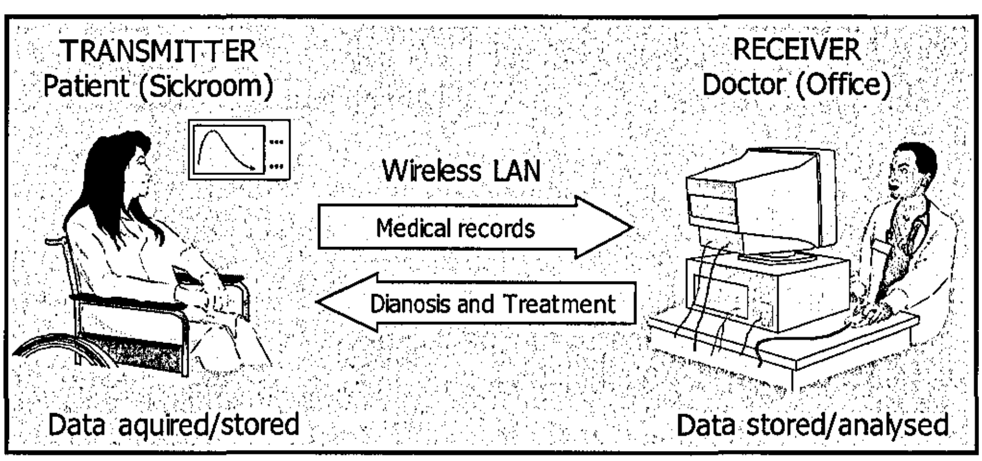


Figure 3. 1 Principle of telemedicine systems

For the mobile patient unit, the functionality is first taken into account. That means, before we start the hardware design, we should make clear what kind of patients we are dealing with, which medical data we are going to send, and how to deal with that data. Secondly, we should think about the mobility. This includes the working time (duration) and portability. Thirdly, the unit should be easy in use. Since the unit is for common use, patients should feel confident to master its usage after some brief training. Finally, the device is produced at a low cost that is affordable by general patients. In a word, a smart-size, full-function, and low-power design is required.

At the service centre, the healthcare system needs to be easily accessible to doctors/specialists to acquire the patients' medical data. We need to build up a database that features in quick response, which relates to efficient data management, i.e., new data update, data retrieval, a rational structure for economical data storage, and a user-friendly interface. Meanwhile, the system should provide convincing data security for patient health status privacy. Finally, the system should be easy to set up and easily maintainable, which is a key problem in the deployment and system life.

Data transmission is essential in implementing telemedicine. It mainly depends on the service type, and the functionality of the mobile patient unit as well. These two targets determine the transmission technology that provides efficiency and accuracy, which means low data rate and reliable communications. Another method to improve efficiency is data compression before transmission. A proper compression method can greatly reduce the data size while keeping the original integrity. Data transmission also provides security, but it is different from the one in the healthcare system, in that the latter focuses on the database access privileges, and it works on data secrecy during transmission, which requests data encryption. Besides, a carefully designed data packet helps with data interpretation in both patient site and healthcare site.

Some research has presented requirements for data transmission, including the PSTN comparable voice quality, different data rates for high-speed moving users and office users, compatibility to Internet communications, support for a wide variety of mobile equipment, and flexible introduction of new services and technologies[41]. In other research, data transmission is divided into two different modes, namely the real-time interactive mode and the store-and forward mode[6]. In the real-time interactive mode, a large amount of information is transmitted in a short time. It emphasises transmission, exchange, and interaction, but its major determinant is throughput (transmission speed and bandwidth). The store-and-forward process tends to move blocks of data at a time and is less demanding in speed and bandwidth requirements.

The overall system requires being reliable and "future-proof", including an extension in services, compatibility in communications technologies, and development in computer assistant tools. Some studies also point out that the cost has been the primary barrier to implementing telemedicine. However, we can still remove this obstacle by introducing new technologies, which are highly developed and integrated, minimising the cost of human operation and function duplication.

In the following sections, we present a system design based on the system requirement we discussed above.

3.2 System Design

3.2.1 System Diagram

Figure 3.2 shows a diagram of the wireless monitoring system that is set up in a hospital. The system consists of four major "components": Mobile Patients in the coverage area of the hospital WLAN, a Hospital Server with a Database, the Healthcare Group, and doctors outside the hospital. The system also allows interaction among hospitals that are running the same system.

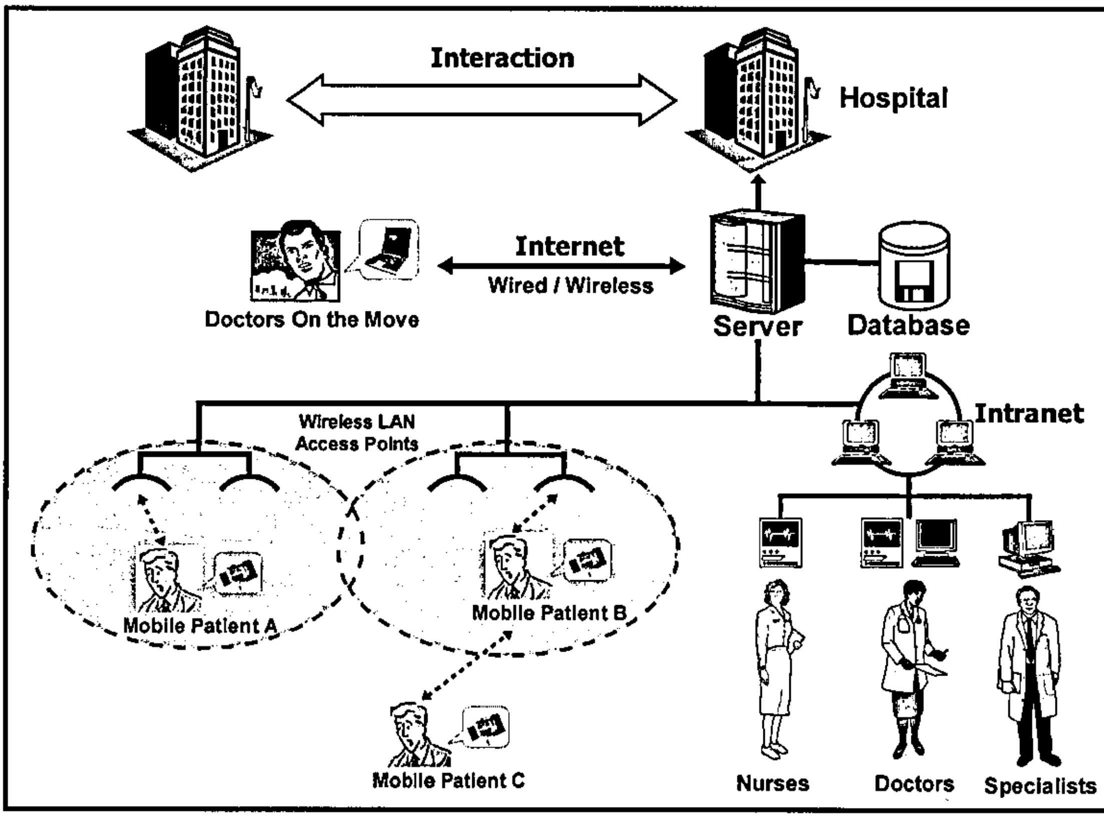


Figure 3. 2 System diagram of a telemedicine system using WLAN technology

1. Mobile Patients

Mobile Patients carry medical devices that work as the data source of the whole system. These devices contain WLAN transceivers that are wirelessly connected to the Hospital Server. The biosensors on the devices sample medical data from the patients and the WLAN transceivers send the data to the Hospital Server. The devices also receive control signals from the Healthcare Group and function accordingly.

There are two types of Mobile Patients. For those within the coverage area of the WLAN Access Points (AP) installed by the hospital, they can connect to the Hospital Server directly and are therefore called "direct patients". For those not covered by the WLAN AP but still within the range of direct patients, they can connect to the Hospital Server via the direct patients and are therefore called "indirect patients", i.e. direct patients are a gateway for indirect patients.

2. Hospital Server

The Hospital Server works as the "brain" of the system, co-ordinating different parts of the system to work correctly. It controls the system functions and performs the database management.

1) It receives and interprets data from Mobile Patients, and then either saves medical records in the database or displays them to medical devices.
2) It retrieves medical records on doctors' demands and generates appropriate displays on their computers.
3) It initiates interaction among hospitals, enabling teleconferences and information exchanges.

3. Healthcare Group

The Healthcare Group provides real time/routine healthcare to Mobile Patients. It consists of nurses, doctors and specialists.

1) Nurses do real time/routine checks on medical devices for Mobile Patients and report emergency cases.
2) Doctors make instantaneous diagnosis on reading real time medical data displayed on medical devices, and make a detailed diagnosis by reading a set of records retrieved from the database.
3) Specialists can give expert opinion on after researching long-term records.

4. Doctors on the move

When doctors are travelling away from their usual workplace, they can still access the Hospital Server via the Internet, so as to provide healthcare, especially for emergency diagnosis and treatment.

3.2.4 System Functions

The whole system functions in three steps.

1. Data sampling and sending

After sampling, the data would normally be sent to the Hospital Server. To achieve this, the medical devices on Mobile Patients can operate in two ways:

1) *Automatic method* – periodic operation: the device automatically samples data from the patient periodically, for example, sampling a 10-minute ECG data every 2 hours. In this case, the data transmission is in the store-and-forward mode.

2) *Manual method* - doctors request operation: the device samples data from the patient at the doctor's request. In this case, the data transmission may be in both the store-and-forward mode and the real-time interactive mode.

2. Getting a solution

When new data is received, it is displayed to the Healthcare Group as well as written into the database, and then a doctor makes a diagnosis. If new cases appear, doctors are required to pass the solution to their patients.

3. Solution for the patient

When a solution is available, a patient could be informed by one of the following two methods.

1) *Automatic method* - signal by medical devices. This needs a protocol between a patient and a doctor. Provided that there are two 8-segment LEDs on the Patient Module, up to 100 cases could be indicated (00~99). Patients check the user manually for an instruction, which in many cases

may be dealt with by patients themselves.

2) *Manual method* - phone calls from doctors. It fits for emergency and new cases but can still be executable by the patients themselves. Patients could deal with the problem step by step following doctors' instructions. If it turns out to be a serious case, the patient can make some preparations while waiting for first aid.

3.3 Design Concept

3.3.1 Characteristics of Medical Data

Table 3.1 describes the electronic characteristics of several typical medical signals. These signals vary a lot in value. However, all of them can be converted into digital data and converted back to analogue signals in the receiver. At the moment, we focus on the transmission of ECG signals because they have the most complicated characteristics and require the most processing for capture, analysis, transmission, and retrieval among the intended medical signals.

Signal	Frequency range	Signal Range
Electrocardiogram (ECG)	0.05 – 100 Hz	10 uV – 5 mV
Heart Rate	45 – 200 beats/min	N/A
Breathing Rate	12 – 40 breaths/min	N/A
Blood Pressure	110 – 130 Systolic 75 – 85 Diastolic	40 – 300 mm Hg (Arterial) 0 – 15 mm Hg (Venous)

Table 3. 1 Electronic characteristics of several medical signals

Willem Einthoven developed ECG monitoring in the early 1900s. It is a method to measure and record different electrical potentials of the heart by placing three or 12-lead electrodes on selected spots on the human body surface[42]. **Figure 3.3** shows an ideal ECG signal with its all elements and complex[42]. The ECG may roughly be divided into the phases of depolarisation and repolarisation of the muscle fibres making up the heart. The depolarisation phases correspond to the P-wave (atria depolarisation) and QRS-wave (ventricles depolarisation). The repolarisation phases correspond to the T-wave.

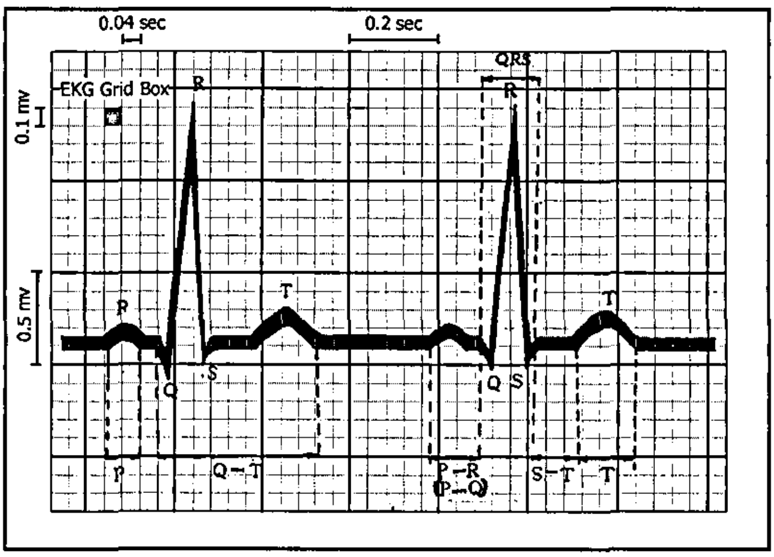


Figure 3. 3 An ideal ECG signal with its all elements and complex

According to Table 3.1, the frequency range is from 0.5Hz to 100Hz. Referring to the Nyquist sampling theorem, a minimum sampling frequency of 200Hz is required.

In consideration of the voltage level in ECG sampling, the requirement of voltage step ranges from 1.25mV to 5mV[43]. Since we are going to develop a 5V level hardware, which is 4,000 times 1.25mV and 1000 times 5mV, we need to use an analogue-to-digital converter (ADC) with the precision between 1000 and 4000, i.e., an ADC with an output ranging from 10-bit (2^{10} = 1,024) to 12-bit (2^{12} = 4,096), or even higher for higher precision.

Therefore, we may use a sampling rate of 250Hz with 12-bit resolution in ECG characterisation processing for our design.

3.3.2 Data Packet Format

Transmitting data that contains medical signals from patients to the database server system is one of the key issues in the whole telemedicine system. This issue could be drawn into what data to send and how to send it, which is essentially the application of the hardware design. "What data to send?" could be considered as "what kind of data should be sent in what format?" Since the required data type depends on doctors' requirements, we now focus on the data format.

It is very important to form a proper data format, which in fact is a protocol between the transmitter and the receiver. A good format makes data interpretation easy, whereas a bad format leads to poor interpretation and data ambiguity, or even errors.

In WLAN and the Intranet, data are transmitted in IP Packets. An IP packet consists of a header and a data section up to 64 k-bytes[37]. In transmission, we include the medical signals in the data section. Then the data is encapsulated into a complete IP packet by adding the header. We cannot do too much to the header as it is set by the TCP/IP protocol. The format mentioned above is the composition of the data section. **Figure 3.4** shows a brief structure of an IP packet.

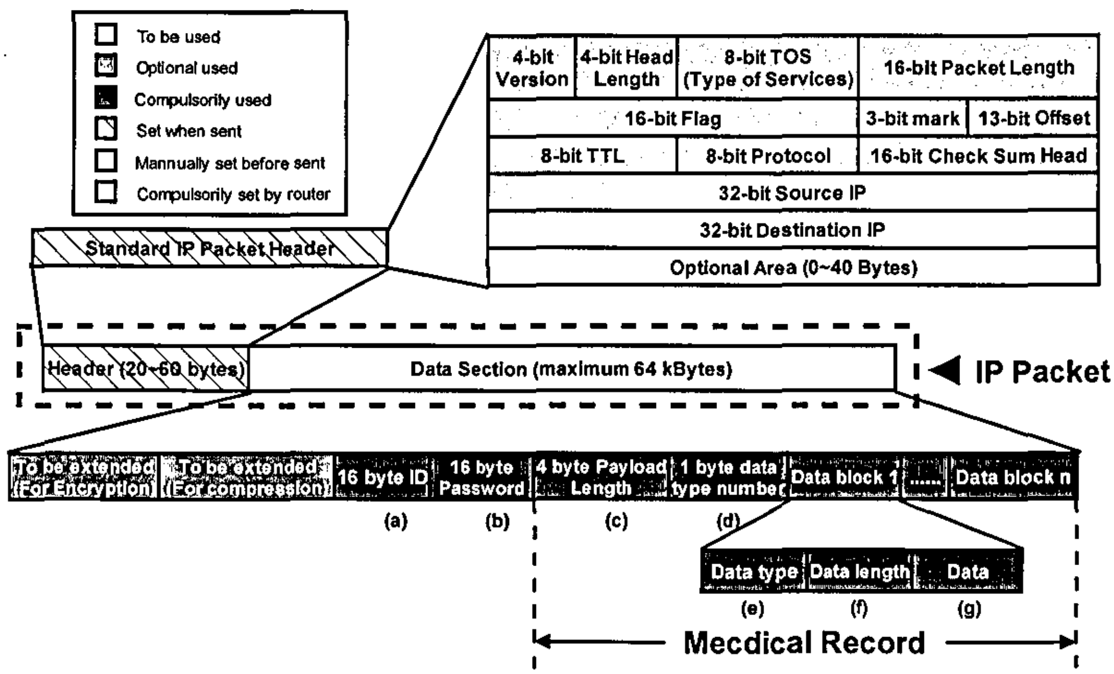


Figure 3. 4 The IP packet structure set for telemedicine

a) 16-byte ID: the unique identification of the mobile module sending this packet. It could be the IMEI number of serial number of the module.

b) 16-byte password: supporting the user identification. It is set by the medical centre and held by the hardware.

c) 4-byte payload length: a check sum to make sure that the server has received a complete and correct packet. It indicates the length of the rest of the data section.

d) 8-bit data type number: indicating the number of different medical signals sections.

e) Data type X: indicating the type of incoming signal. For example, we define "1" as an ECG, "2" as blood pressure, "3" as body temperature, and "4" as SpO_2.

f) Data length X: indicating the length of the transmitted data.

g) Data X: the actual signal.

This format is flexible, effective and efficient. No matter what kind of data and how much data is sent, we could arrange it to the fixed format. The "Type-Length-Data" format makes the data easily interpreted by the receiver. Besides, the format is extendable in future developments. If we want to add a new kind of signal, we just make the changes in the data type sorting, without changing the format.

In some future steps, we may make tiny changes to the format by adding some new columns, when we need to do the data encryption and compression. However, the main format is to be maintained.

3.3.3 System Security

Telemedicine requires providing data security for patient records, including the user access rights to the database server that are assured by user authorisation, and data privacy during transmission and validity when received by the Hospital Server, which needs a special transmission method. The system security is implemented in the following aspects.

1. Authorisation Methods

Users of the telemedicine database, including both doctors/specialists and patients, are required to be authorised when they access the database. With different identities, they are granted different privileges, such as writing, reading, and deleting, etc, to different records in different storage area.

For doctors/specialists, they just log into the server manually via the doctor browser with their unique IDs and private passwords when they access the database. Then they are allowed to read patient records, write down their diagnosis records, and delete some improper diagnosis.

At the patient site, the data transmission and interpretation is transparent, which would be discussed in detail in Chapter IV. Hence, patient authorisation is also automatic and transparent. In this case, we pack the user ID and password into the packet before transmission. The server reads the ID and password to perform patient authorisation.

There comes the security problem. Patients have the privileges to update their records in the database. That is, to delete old records and write new records into the database. It is necessary to provide high enough secrecy to the patient packet during transmission. A solution combining the ***encryption*** and ***compression*** is presented in detail in Chapter VI.

2. Encryption Issues

In Section 2.3.4 we discuss the WLAN security provided by the WEP encryption, which only works during the wireless transmission. To provide the security that covers the entire telemedicine system, we should perform another data encryption at the patient site before sending the data. The procedure is described in **Figure 3.5**.

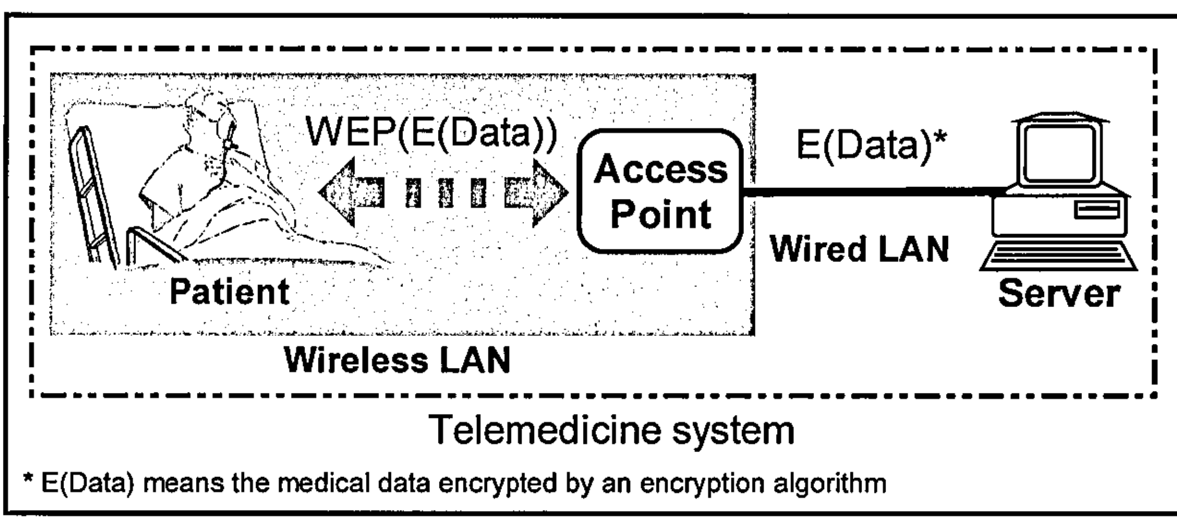


Figure 3. 5 The encryption procedure of a medical record

In choosing the encryption algorithms, the secret key (symmetric key) cryptography is taken into account due to its much higher efficiency than the public key cryptography, which is suitable to encrypt the large amount of medical data. Currently three of the most popular algorithms are the 64-bit key DES, the 128/192-key Triple DES and the 128-bit key AES. The latter two algorithms provide much higher security than DES, but they take at least twice as long as DES. Considering the hardware device is working at a low CPU frequency of around 40MHz we chose DES, which performs much faster and provides high enough security together with WEP. **Figure 3.6** describes the overall scheme of the DES algorithm[44].

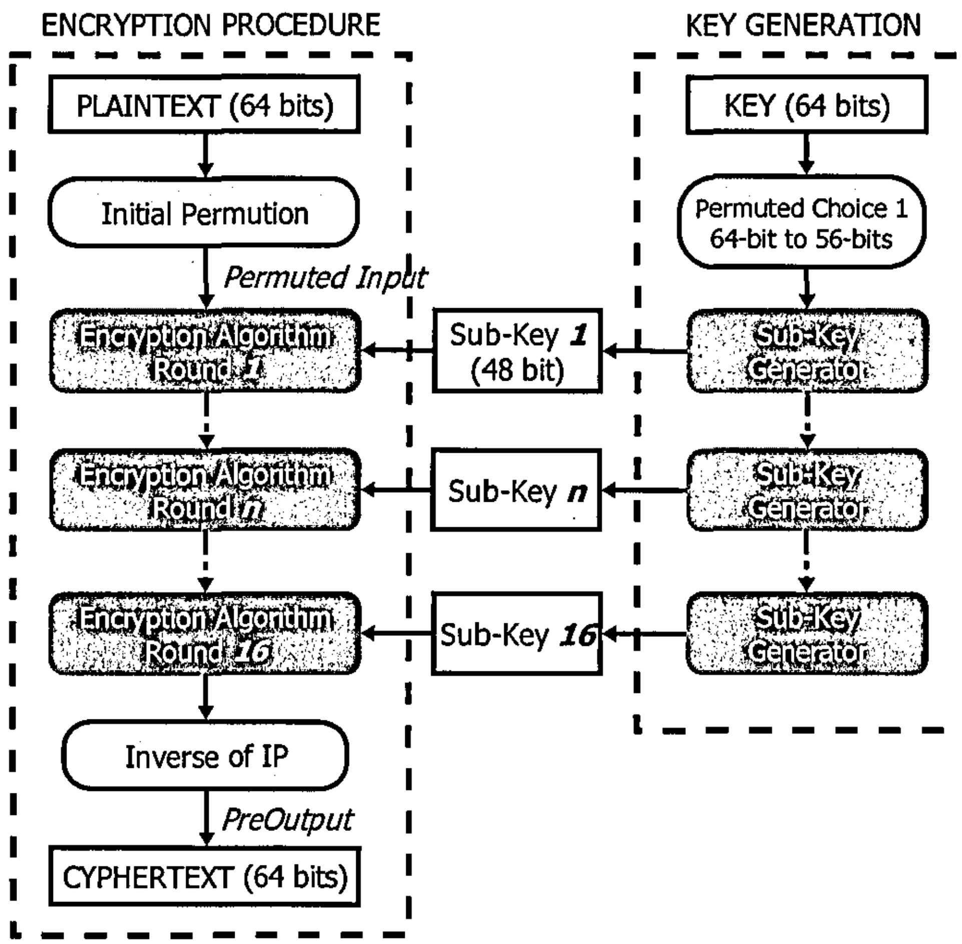


Figure 3. 6 The overall DES algorithm

In DES, a block of 56 bits is selected from the 64-bit key and generates 16 groups of 48-bit sub-keys. These sub-keys respectively encrypt the 64-bit plain text in a 16-iteration encryption algorithm and finally output a block of 64-bit cipher text.

In encrypting the medical record, the plain record is divided into a sequence of 64-bit blocks and encrypted sequentially. The output cipher blocks are reunited into the cipher record with the same size as the plain record. This procedure is shown in **Figure 3.7**.

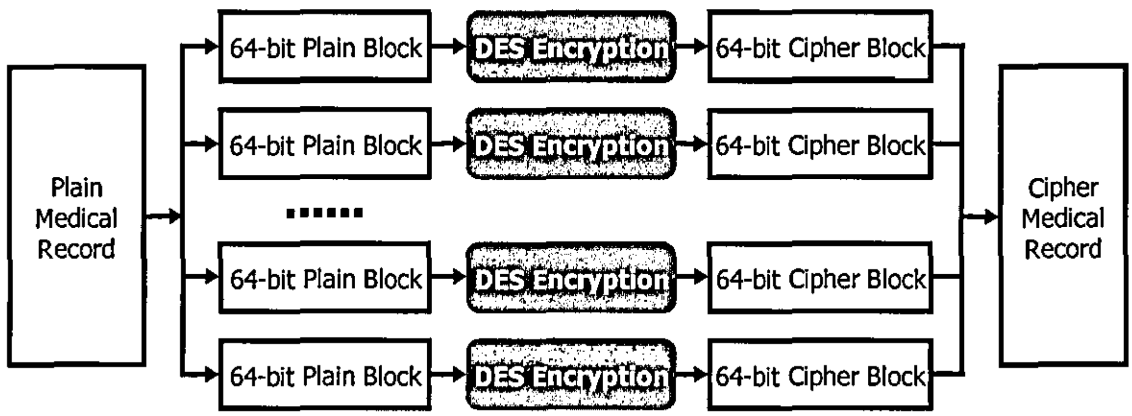


Figure 3. 7 The encryption procedure of a medical record

3. Compression Issues

Compression is an effective method to reduce the size of the medical record, so as to reduce the transmission time. Some projects use MPEG-2 to compress video records and JPEG-2000 for image records according to Digital Imaging and Communications (DICOM).

In our project, the input data sources are digitised bit-streams converted from the analogue sensors, and transferred into proper format displayed to doctors at the hospital site. Therefore the lossless Huffman compression is adopted. The coding algorithm of Huffman is available in [45].

CHAPTER IV

HARDWARE DESIGN AND SOFTWARE IMPLEMENTATION

4.1 Conceptual Hardware Design

4.1.2 A Modular Hardware Design

As shown in **Figure 4.1**, we divide the whole hardware system into two main parts: a fixed control module and a changeable application module. The control module works with different application modules, stores the data and transmits the data to medical nodes. Each application module may be designed for a special purpose, for example an ECG sensor unit gets the ECG signals; or for multiple purposes, such as a unit integrated with biosensors for ECG, BT and BP. It mainly defines the function of the whole system. The connection between the control module and the application module is discussed later in this section.

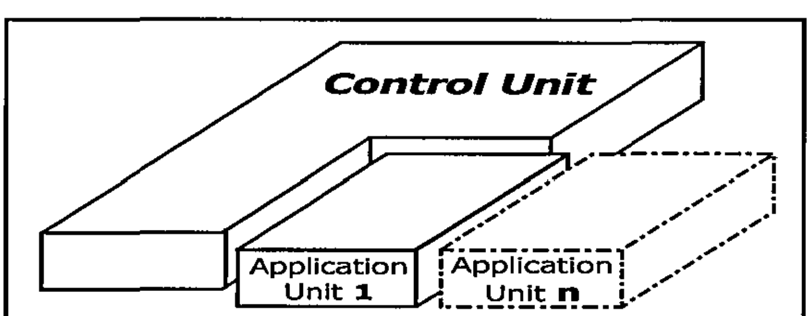


Figure 4. 1 A modular hardware design

This kind of design conception benefits a lot as following:

1. High Functionality

In this system, the control module is unchanged but the application module is alterable. With different application modules, the whole hardware system could implement different functions. For example, with the same control module, we can provide a diabetic unit to diabetics, while we can provide heart-disease unit for heart disease patients, and so on. Therefore, we produce various application modules for various requirements, rather than integrate all functions in one board. It is also acceptable for patients, as they don't need to pay for some un-used functions.

2. Simplified Implementation and Interference Immunity

Physically separate circuits simplify the design, debugging, and updating of circuit boards. We can focus on the components of each single module, without being bothered by larger numbers of chipsets and the more complicated wired circuits, which shortens the design period and enhances the hardware reliability.

The modular design is also immune from in-module interference. It avoids the interference between high and low frequency signals, analogue and digital blocks, and high-density signal and power wires, which also increases reliability.

3. Easy and saving in manufacturing

As is mentioned above, the system has an invariable control module and a convertible application module. In this case, when a new challenge comes, the only thing we need to do is to design a new application module, and to update the software in the control module, without changing the whole hardware system.

4.1.3 Hardware Design

Figure 4.2 shows the hardware design diagram. We can see that there are four main units: a micro-controller system, a WLAN transceiver, a biomedical sensor unit, and a unit for further improvement. They function as the follows:

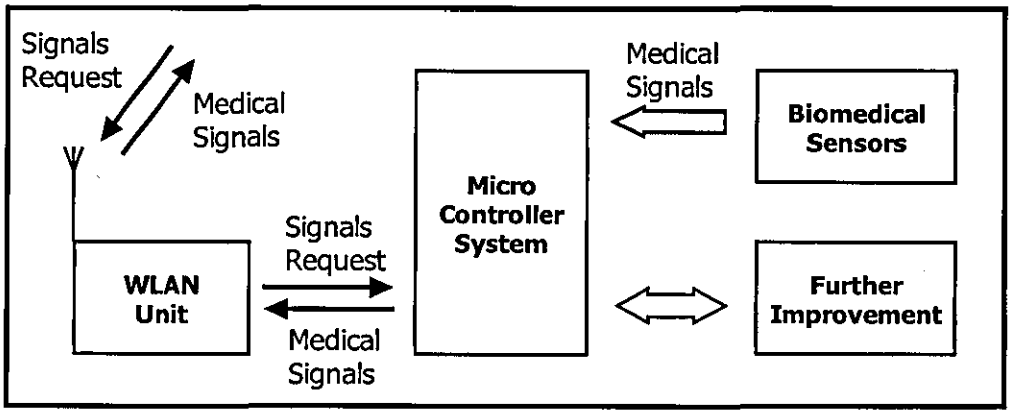


Figure 4. 2 Hardware design diagram

1) Specific biomedical sensors sample biomedical signals periodically as required and send them to the micro-controller system where the signals are interpreted and stored.

2) When the WLAN unit receives the request for signals from the healthcare system, it passes the request to the micro-controller system.

3) The micro-controller system packs the medical signals together with data handling, and sends them to the healthcare system via WLAN.

1. The Micro-controller System

The schematic diagram of the micro-controller system is shown in **Figure 4.3.** It contains a *microprocessor*, an *interface control unit*, a *SRAM (Static Random Access Memory) unit*, an *on-board programme unit*, and a *user operation unit*.

The *microprocessor* is the "brain" of the system. It controls all other modules in this unit. It executes data and allocates data to different modules. Its main job is: 1) to receive medical data from the biomedical sensors via the outer interface; 2) to control the WLAN module to send or receive data; 3) to store medical data into the SRAM array; and 4) to process the re-programme operation.

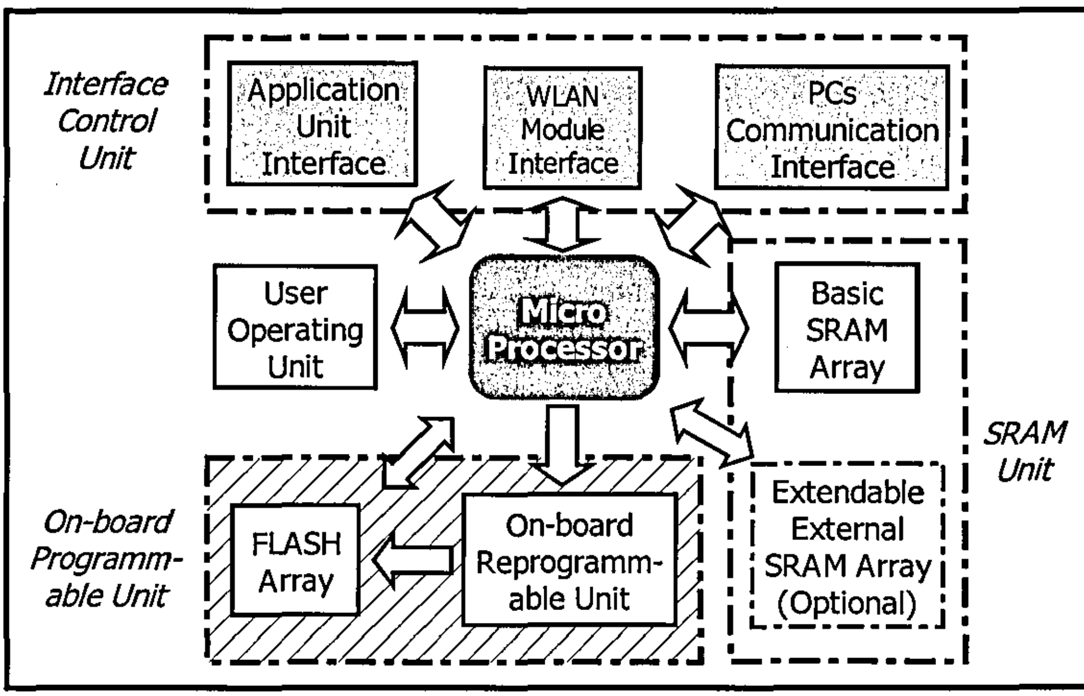


Figure 4. 3 The schematic diagram of the micro-controller system

The *on-board programme module* consists of an on-board re-programmable unit and a FLASH memory array, which stores the system programming codes. The programme module plays a very important role in the system operation and system update. It has two function modes: the common mode and the re-programmable mode. In the common mode, the microprocessor reads the programming code from the FLASH array and runs accordingly. In the re-programmable mode, the microprocessor refreshes new codes into the FLASH array via the on-board re-programmable unit.

The *SRAM unit* contains a *basic SRAM array* and an *extendable external SRAM* *array.* The *basic SRAM array* provides the basic storage room for medical data. Its size should be considered seriously, which mainly depends on the amount of medical data. In our project, an ECG signal would decide the SRAM capacity. For a 10-minute ECG signal, if we sample at 400Hz with the 12-bit sampling precision, which would be stored as 16 bits per sample, the memory size needed can be estimated by:

$$\begin{aligned}\text{Total Data} &= \text{Sampling Rate x sampling precision x Duration} \\ &= \text{400 samples/s x 16 bits/sample x 60s/min x 10min} \\ &= \text{3.84 Mbits}\end{aligned}$$

Therefore at least four-mega bits SRAM size is needed in this case.

A flexible scheme to meet further needs in the future is the *extendable external SRAM array.* That is, we reserve the interface in the microprocessor for external SRAM array.

The *interface unit* provides interfaces between the micro-controller system and other units/modules. The *WLAN module interface* links the WLAN transceiver to the microprocessor. It mainly works as an adapter that fits the voltage and current level, as well as data- transmitting rate and data format. It ensures the validity of the data transmission between the two parts. The *application module interface* is a universal interface, either wired or wireless, to the application modules. The *PCs communication interface* is a wired interface for the communications between personal computers and the hardware. This interface is mainly used for on-board reprogramming of the hardware.

The *user operating unit* is used for user control to the hardware. It may contain a LCD or 7-segment LEDs for instruction to the user, and several buttons for operations.

Based on the discussion above, a AM186ER microcontroller produced by Advanced Micro Devices, Inc. was adopted. It has the following key features:

1) 32 Kbytes of integrated RAM
2) 100 pin PQFP and TQFP packages
3) 50 MHZ maximum frequency = 6.6 MIPS
   - 5V tolerant I/O
   - TTL compatible
4) DMA to/from asynchronous serial port
5) Hardware Watchdog Timer

2. WLAN transceiver

Designed with the WLAN technology, this unit could access the Internet using a wireless link. Hence, it could send the data from the micro-controller system unit to other computers on the Internet, or receives data from the Internet and transmit them to the micro-controller.

We chose to embed a WLAN module/chipset to the circuit for our design, rather than linking the hardware to an expensive PDA with embedded or plug-in WLAN products. That may significantly reduce the cost, and besides, freeing the patients from PDA operations and enhancing patient mobility.

We chose a WLAN transceiver compatible with IEEE 802.11a/b/g, in which 802.11b is currently the most popular in use, and 802.11a/g are new protocols the would be applied and deployed as the replacements of 802.11b in future, which allows the hardware for long-term use.

Currently there are several kinds of WLAN modules. They are:

Existing products with universal interfaces such as PCMCIA and USB. Usually these modules provide full WLAN services and we could use them directly by plugging it into relevant universal interfaces. However, it would be uneasy to work with the software embedded in the module. Considering the simplicity, we take the USB module as the first option for our design.

Modules for further designs. These modules need further development to become complete WLAN transceivers. Some of them with universal footprints, such as BGA, could be soldered onto the circuit directly, while some others have universal interfaces, such as CF and SD. This kind of modules is easy to control and low cost, but it needs hardware extension, such as the antennas. They are good choices for final products in applications in the future.

3. Biomedical Sensors Unit

This unit works as the data source of the entire system. We do not care how it works since it mainly works as a black box to us. We just need to make clear the data type, to receive the data and transform them into a proper format, and to store them into the SRAM array.

4. Further Improvement Unit

This unit is designed for the purpose of future improvement. For the sake of compatibility, we may adopt a universal interface.

5. Hardware Modularisation

We now modularise the hardware structure of Figure 4.2 into **Figure 4.4**. The control module contains the micro-controller system and the WLAN transceiver. It mainly receives data from the application module, stores or processes the data, and sends the data to the Hospital Server. The application module includes a biomedical sensors sub-unit and a further improvement sub-unit. Different application modules function for different specific purposes. These two types of modules are connected by

PC-compatible universal interfaces, such as the USB port, serial port and the parallel port, which will be discussed in the next subsection.

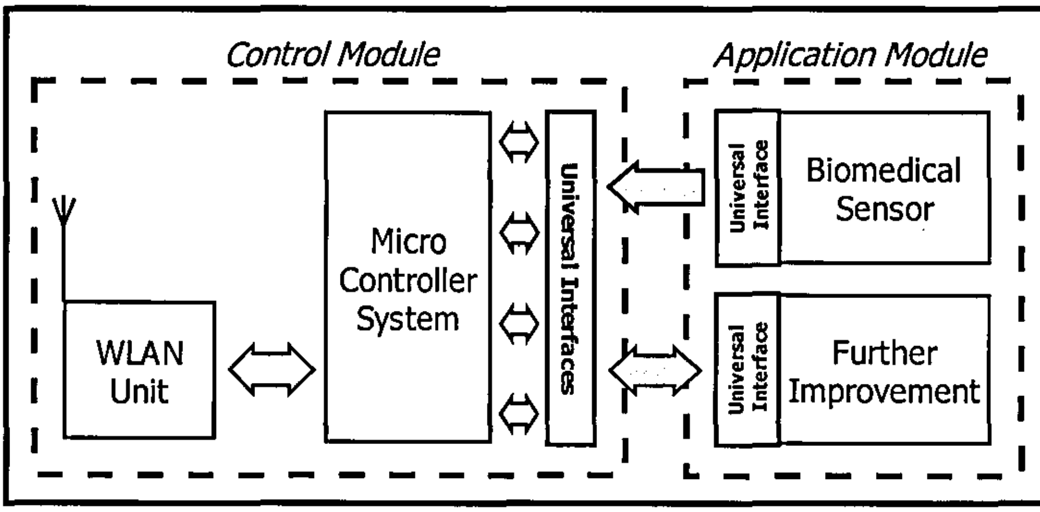


Figure 4. 4 Hardware Modularisation

4.1.4 Module Communications

1. The connection interface

We focus on the following universal interfaces that are the most widely in use. They benefit in easy design and compatibility with computers and peripherals.

1) USB

The high-speed USB (Universal Serial Bus) is the first option. The USB1.1 standard provides a data rate up to 12Mbps, and for the latter standard USB2.0 a much higher 480Mbps is available, which fully fulfil the needs of telemedicine. However, if we choose a USB WLAN module, we could not build up a USB connection, because seldom microprocessor provides dual USB ports on chip. Besides, the relatively more expensive USB-embedded microprocessor may increase the cost of the system.

2) Serial port communications

This communication is common and simple. But for some microprocessors, they provide the transmitting data rate ranging from 9,600 bps to 38,400 bps, which limits the functions of both control module and application module.

3) Parallel port communications

Compared with the serial port, it provides a data rate up to 384kbps and easy configurations. The main drawback is the thick heavy parallel cable, which limits patient's mobility.

2. The connection protocol

There are different application modules that may implement different functions and hence the control module should work in different ways. So the control module needs to "recognise" the application module at the time the connection is set up. **Figure 4. 5** shows a protocol for these two modules.

1) At power on, the application module sends a byte as its Module Serial Number to the control module. For example, "1" as ECG sensor, "2" as blood pressure metre, etc.

2) When it receive the Module Serial Number, the control module sends back a relevant Serial ACK (acknowledgement) as a response. For different Serial Numbers, the ACKs are different.

3) The application module judges the validity of the ACK.

4) If the ACK is valid, the application module sends back the ACK as confirmation, then both the modules are initialised.

5) If the ACK is invalid, the application module sends an "ERROR" to the control module. Then the control module alarms for the error and both the modules stop.

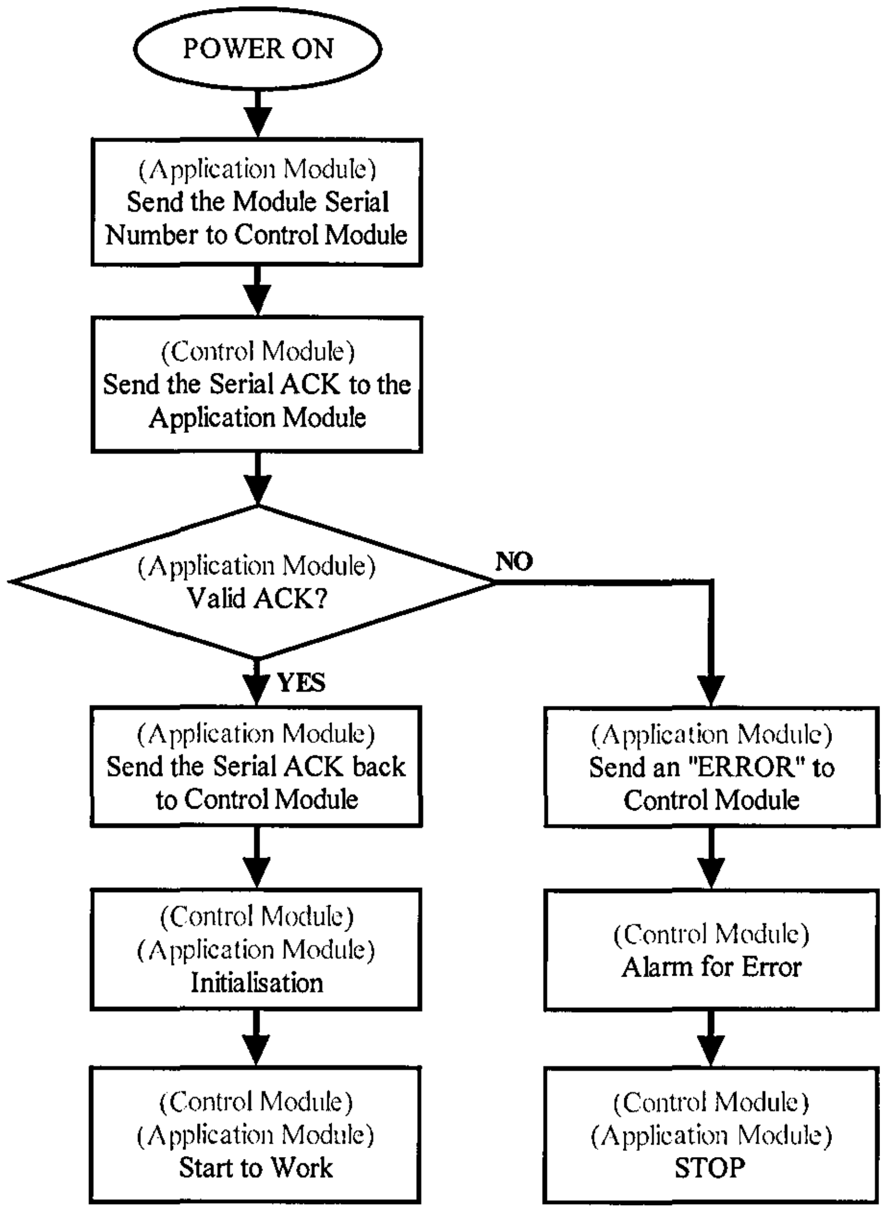


Figure 4. 5 Flow of the module communications protocol

4.2 Software Design

The software design of the system is structured in four main elements:

1) Designing, manipulating and running a database in the MySQL database server,

2) Designing the database interfaces for both doctors/specialists and mobile patient modules,

3) Discussing the communication between mobile patient modules and the database,

4) Programming simulation software of the hardware to test the whole system. The implementation of all this work ensures good preparation for the hardware design, because the hardware should now be able to function with them as an essential part of the project.

4.2.1 MySQL Database

MySQL is a client/server-structured database. When the MySQL server is running, it allows clients to access from either a local host machine or a remote host machine via the Internet or the intranet. It is both easy to operate and powerful. It responds to all sorts of query operations, such as retrieving, adding, deleting and updating data, and returns corresponding results in suitable user views[46].

We build the database with the structure shown in **Figure 4.6**. Each table represents a physical block of storage and the boldface is the table name. The items inside are the chief attributes. The arrows represent the relationship between different tables.

The *Doctor Table* stores doctors' working information, such as their IDs, names, departments, working areas, and contact numbers, etc. The *Functionary Table* and *Medical Condition* set up the relationships between doctors and their patients and the patients' health problems, so that we could list the patients listed by both their doctors and diseases.

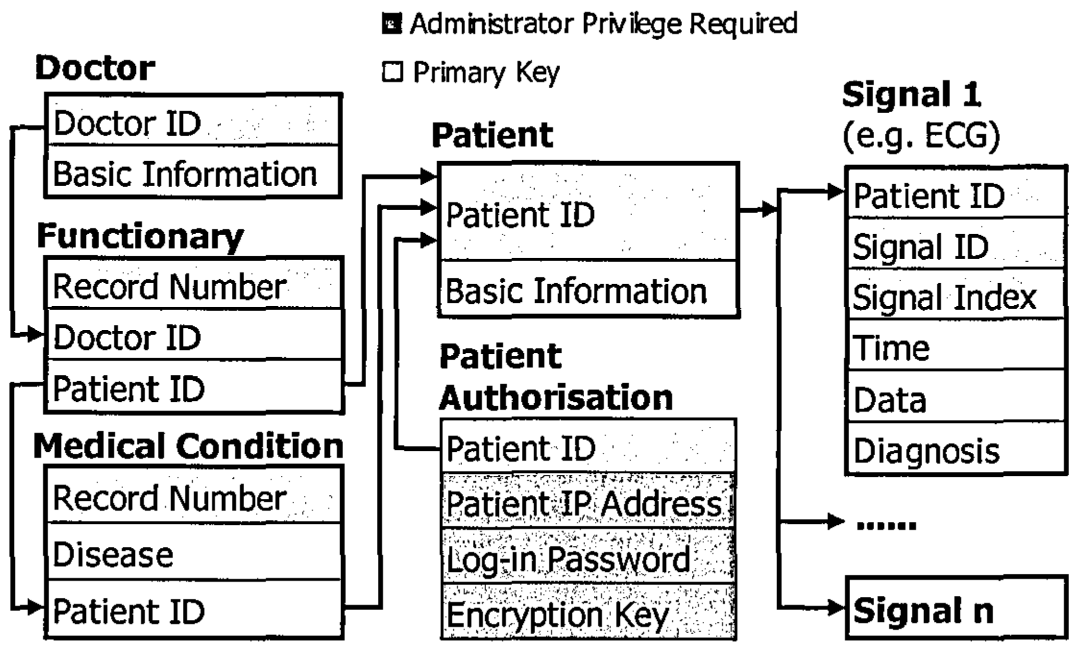


Figure 4. 6 Physical structure of the database

The *Patient Table* contains the patient records, such as IDs, names, address, and contact numbers, etc. The *Patient Authorisation Table* is for medical signal transmission security use with administrator privileges. Since medical signals are transmitted transparently, mobile patient modules access and update patient records automatically via the Local Interface (LI) in the server. For security reasons patient authorisations are required. Supposed that patients have fixed IP addresses, they can log in to the server only when the data packets contain their IDs and correct passwords from the specific IP addresses.

The *Signals Table* stores patient medical records that are stored in segments by categories and could be retrieved with both Signal IDs (names) and Signal (segment) Indexes. With certain patient IDs, doctors can obtain patient records and record their diagnosis for each segment.

For doctors with unique ID numbers, they can list all their patients' IDs from the Functionary Table. Each doctor can access their patients' data from the

Patient Table, then medical signals from the Signals Table. The doctor can also get the list of Patient IDs by their medical status from the Medical Condition Table, which is useful for medical statistics.

4.2.2 A Two-Interface Database Structure

In the complete database server system, we have a two-interface scheme, which involves a *Local Interface* (*LI*) for mobile patient modules and a *Remote Interface* (*RI*) for doctors, as shown in **Figure 4.7**. The former works at the

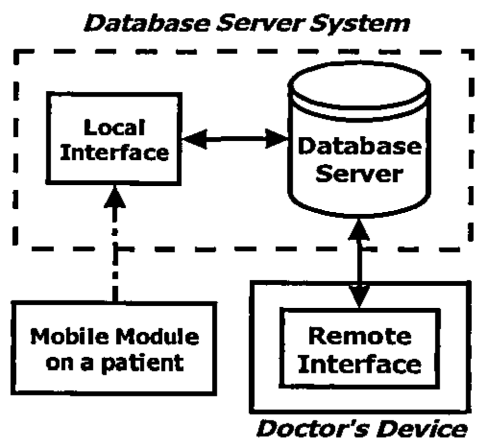


Figure 4. 7 A Two-Interface Database Structure

database station, receiving and interpreting medical data from remote patients, as well as loading the interpreted data into the database. The latter interface works at the doctors' station, such as PC, laptop or PDA, letting users access the database. In this subsection we will discuss the LI and the RI in detail.

1. The Local Interface

As mentioned before, the MySQL database system typically uses the query language to carry out different tasks. It can only respond to different sorts of queries from users, but cannot deal with any data automatically. Thus, when the database system receives a data packet with a format shown in Figure 3.6, it is unable either to extract any data into different types, or to answer any queries. In this case, we need to build an "adapter", which not only interprets data packets, but also makes corresponding database operations.

Once the LI receives a data packet, it works as follows:

(a) Obtains the source IP address of the packet and extracts the first 16 bytes, the user ID, and subsequent 16 bytes, the user password, with which the LI checks the user's validity.

(b) Extracts subsequent four bytes to make sure that the LI has received a complete and correct data packet.

(c) Extracts the next one byte to get the number of all data types included in the packet.

(d) Extracts all sets of data, and loads them into relevant tables according their data types.

(e) Logs off the database system.

All the transactions above are automatically completed by a computer, which means they are transparent. However, the DBA (database administrator) can view these steps via the GUI (Graphic User Interface).

2. The Remote Interface (RI)

Some researches present the idea of web-based monitoring, enabling the live broadcast of medical signals over the Internet, and displaying the signals to doctors on the website[47, 48]. The idea features in easy access of medical records, but does not support data download and local data management on a doctor's device.

In our system, the RI is software installed in a device controlled by a doctor, such as a PC, laptop or PDA. It helps doctors to access the database system easily. Unlike the LI, the RI is user-friendly software with an easy-to-use interface. Instead of typing complicated query instructions, doctors simply perform their operations by choosing several options. The software then converts the options into corresponding query languages, and returns the result in a format that is understandable to doctors. For example, the ECG signals are shown as moving graphs, and body temperature signals are decimal numbers, just like the results on the traditional medical devices.

In using the RI, a doctor holds a valid user ID, and accordingly he is granted a certain level of access. On the one hand, he has the "read privilege" to obtain his patients' information, including the basic information (full name, address, etc) and medical records. On the other hand, he has the "write privilege" to write down useful information, including changes to information (address, telephone numbers, etc), but also any diagnoses for his patients. All these privileges are set at the time the database system is prepared.

4.3 Telemedicine Security

The security of medical records is a serious problem in telemedicine, especially in the open wireless environment. This problem could be divided into two aspects: privacy in transmission and reliability in reception. Privacy means that the information of the packet is unavailable for any eavesdroppers, which is achievable by encryption[49]. Reliability means that the received packet at the server should be exactly equal to the original packet from the transmitter. The RC4 algorithm of WEP provides an integrity check in WLAN, ensuring the reliability of any transmitted packets. However, WEP only covers the WLAN transmission, whereas our goal is to set up a reliable telemedicine network including the Internet, but WEP is still not secure enough either.

In this section, we present a transmission method that contains both encryption and compression, which overcomes the drawback of current security systems.

4.3.1 Drawback of Current Security System

Symmetric encryption ensures the privacy of the patient medical record. If an illegal user receives a piece of encrypted record without a correct key, he cannot decrypt it into the original record, i.e., he gets zero information of patient status from the received record. However, record validity is also requested in telemedicine. It is necessary to identify the transmitter, especially in the Local Interface (LI) of the database server, where the data process and user logon are transparent.

In our system, we adopt a packet format as shown in Figure 3.6, and encrypt the packet with the data encryption standard (DES), so that the packet is transformed into a cipher-text. However, since the format is invariable and the 16-byte user ID and password are unchanged in a certain period, the first 32 bytes of the cipher-text remain the same due to the feature of *block cipher* in symmetric encryption. For example, if a patient with his ID "*PatientID0000001*" and password "*PatientPassword1*" transmits his medical record "*PatientRecord1*", when the encryption key is "*Key00001*", we have the following procession in **Table 4.1** at the mobile patient module:

	16-byte ID	16-byte Password	Patient Record
Plain Text	PatientID0000001	PatientPassword1	PatientRecord1
Hex	50 61 74 69 65 6E 74 49 44 30 30 30 30 30 30 31	50 61 74 69 65 6E 74 50 61 73 73 77 6F 72 64 31	Hex (PatientRecord1)
	50 61 74 69 65 6E 74 49 44 30 30 30 30 30 30 31	⇩ **DES** *(Key=4B 65 79 30 30 30 30 31)*	
Cipher Text	PatientID0000001	0F 5A 6F F0 4F 18 3D 38 C2 27 16 1D 61 17 F0 84	E (Hex (PatientRecord1))
	← *Unchanged 32 bytes* →		

Table 4. 1 Drawback of DES encryption in the system

At the LI, we have a reverse procession so that we acquire the patient ID and password. In an eavesdropper's point of view, the unchanged first 32 bytes of the cipher-text seem to be a free gift. If he simply copies these bytes, regardless of what the original text is, he can pass the identification at the LI and upload whatever he wants to the database, but apparently, the record is invalid, which may cause accidents in diagnosis and the crash of server in record interpretation.

Hence, the security method needs to be changed, either the encryption procession or the packet format, or even both. A practical solution is to randomly change the position of the password every time, and add a cursor pointing to its position in the packet. The LI decrypt the cursor to obtain and decrypt the password. However, this solution does not change the content of the password, which is still not secure enough.

On the other hand, the encryption procedure is time-consuming, especially for a microprocessor with a maximum 40MHz crystal on the patient module. In this case, data processing and transmission efficiency based on data compression seems reasonable.

4.3.2 A Secure and Efficient Transmission Method

According to the discussion above, security requires the frequent change of both the content and the position of the patient password, and efficiency requires reducing the packet size without any information loss, i.e. to use a kind of lossless compression. The main principle of both encryption and compression is to transfer blocks of bits into some other different blocks of bits by using some certain algorithms. For example, Huffman compression reduces the packet size by replacing the bytes that exist frequently with a smaller number of bits, and the infrequent bytes with more bits, which reduces the total number of bits.

In this case, we take the patient password as part of the medical record, i.e. we process both encryption and compression in the patient password together with the medical record. Due to the inconstant content of the medical record, the coding method, such as Huffman tree in Huffman coding, differs each byte of the password in different packets. What is more, it is required to include the compression coding method in the packet to enable the decompression in the Local Interface (LI) at the database server. The variable length of the coding method also practically changes the position of the compressed password. Finally, we encrypt the coding method and the compressed password and medical record, and attach the encrypted text to the plain patient ID. **Figure 4.8** describes the format and coding process of a packet and **Figure 4.9** is the flow chart of the procedure of packet formatting and coding in the mobile patient module.

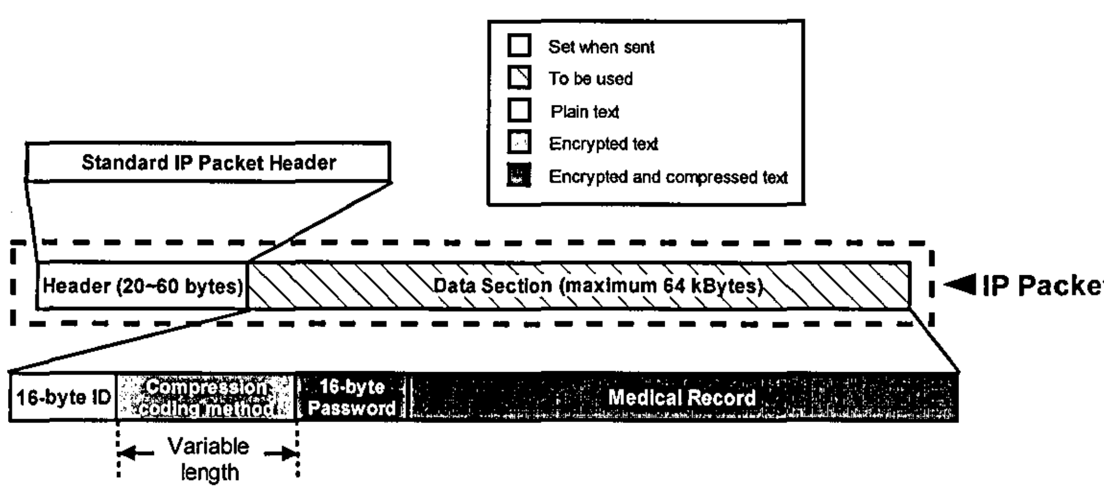


Figure 4. 8 A packet format for encryption and compression

It is more complicated at the LI in the database server because it requires an administrator privilege to retrieve the unique encryption key for a specific patient from the database. Therefore, it is necessary for the LI to log into the database as an administrator to query the key with the 16-byte patient ID before it interprets the received packet. Thereafter the 16-byte patient password is available. Then the LI logs out of the database and re-logs in as a patient with the patient ID and password. If it logs in successfully, it goes on with the data interpretation, or else it drops the whole illegal packet, so as to save time. **Figure 4.10** shows the flow chart of the packet decoding and interpretation in the LI of the database server.

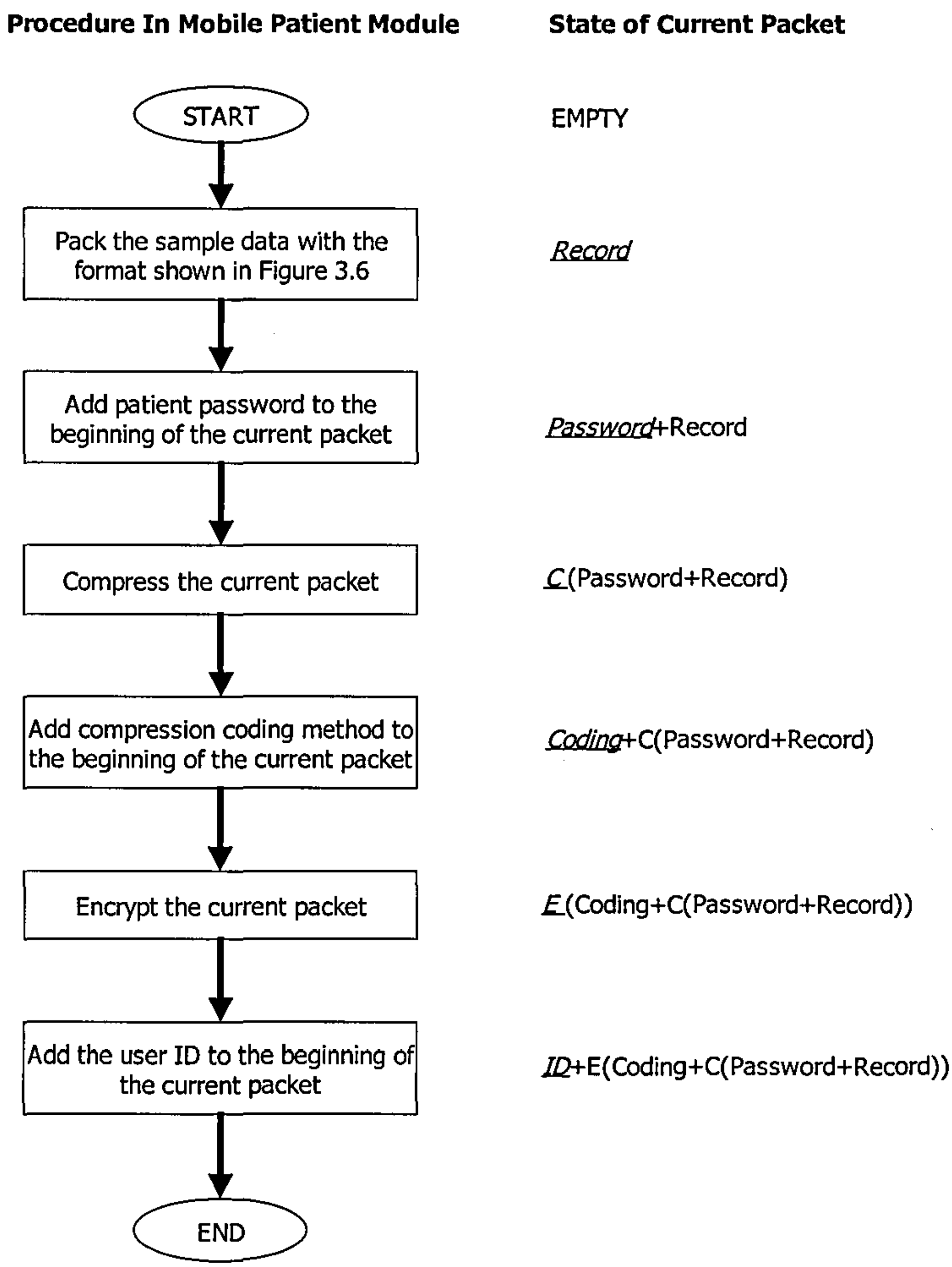


Figure 4. 9 The procedure of packet formatting in the mobile module

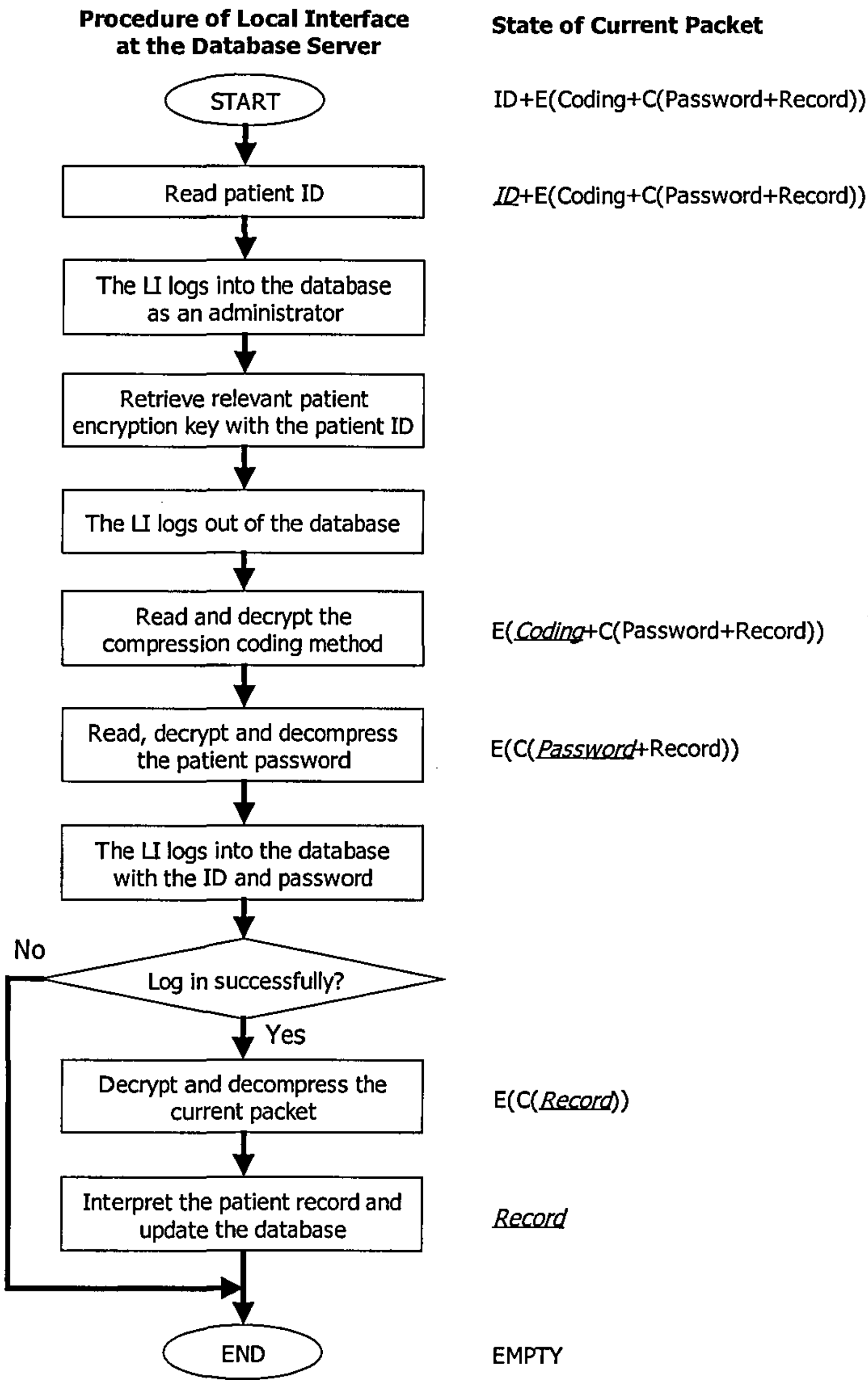


Figure 4. 10 The procedure of packet interpretation in the LI

CHAPTER V

CONCLUSION

5.1 Discussion and Summary

There is a need for telemedicine to provide routine healthcare services for patients who need daily monitoring. Considerable research and many useful applications have proved and illustrated its potential, especially with the development of telecommunications technology, which has lead to the important area of wireless telemedicine.

This thesis presents the following main points:

1. We design a telemedicine system for patient monitoring in the hospital area using the WLAN technology. It features high-speed data rates, low cost, and compatibility with IP networks. A major drawback is the restricted speed of mobile patients within a limited area of roughly hundreds of metres around the fixed WLAN Access Points.

2. The modular design of the control module and application modules in hardware design of the system gives the mobile patient unit flexibility and functional extendibility. For prospective new applications, we only design an individual relevant application module with a universal interface and update the main programme installed in the central processor unit without having to change the whole design. The programmable microprocessor enables future service upgrades by simply linking the central processing unit to a personal computer. The use of a WLAN module/chipset may significantly reduce the entire project cost compared with implementations

with PDAs. The future-proofing design for external memory can meet the requirements of potential services.

3. In software design of the system, we design a multi-thread server that is capable of serving as many users as needed at the same time. The effective database structure can avoid data redundancy and information loss, saving memory storage in the server device and ensuring correct data retrieval. The specific data packet format for data transmission between patients and the server standardises the data interpreting process, making it accurate and efficient, and gaining improvability for new medical data.

4. We design two different interfaces of the database server respectively for patients and doctors. The Local Interface (LI) that is installed at the server site receives patient records, interprets them and updates the database. The Remote Interface (RI) is a doctor browser. It retrieves patient records from the database and displays them in the acquaint format to doctors.

5. We provide high security to the system. Doctors and patients use different authorisation methods to keep out illegal access when accessing the database. Patients are authorised by the LI with the patient ID and password that is contained in the data packet, while doctors are required to log in to the server with their unique passwords via the RI.

6. A data handling method for medical records is presented to assure the data secrecy during transmission and validity when received by the database server. On the other hand, the compress minimises the packet size and shorten the transmission time, enhancing the transmission efficiency.

5.2 Further Implementation and Improvement

Based on the software of the simulation for the Mobile Patient Device, we may next focus on the hardware implementation step by step:

1) Implement the design of the central processor unit and an application module for ECG sampling.
2) Build up a reliable WLAN connection between the Mobile Patient Device and the personal AP, acquire ECG data routinely, and send it in store-and-forward mode.
3) Test the performance of the whole system
4) Complete the data handling.
5) Design the external memory array and re-programmable unit.

5.3 Future Directions of a WLAN Mobile Telemedicine System

5.3.1 3G-WLAN Interworking

Currently the 3G networks support high mobility and universal roaming within a wide coverage area, but sometimes the comparatively low data rate fails to meet the requirements of their subscribers. On the other hand, the WLAN is capable of providing high-speed IP services, but it restricts users to the area around the Access Points.

One good solution to make good use of their advantages is to combine these to networks, i.e. the 3G-WLAN interworking. According to the level of integration required between the two systems, ETSI Project Broadband Radio Access Networking (BRAN) presents two solutions: tight and loose interworking [50].

1) Tight interworking: the WLAN radio interface is used as the bearer of the

UMTS with all network control entities in the core network integrated.

2) Loose interworking: the network is integrated without changing the WLAN standard. There is no need to build a convergence layer and it benefits from easy implementation.

For a telemedicine system built upon the 3G-WLAN inter-networks, it can utilise the broad bandwidth of the WLAN to transmit the large size packet of medical data at the hot spots, and achieve roaming with the global coverage of the 3G systems. As a result, more freedom and better services are available to patients.

5.3.2 WiMAX

The WiMAX (World Interoperability for Microwave Access) Forum was formed to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE* 802.16 and ETSI* HIPERMAN standards, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications[51].

The 802.16a standard is a Wireless Metropolitan Area Network (MAN) technology that will provide a wireless access for the "last mile" broadband. It will also be used to connect 802.11 hot spots to the Internet [52].

WiMAX benefits from the following advantages [53]:

1) Inter-operable equipment cuts the production cost and enables last-mile broadband deployment wirelessly while remaining complementary to Wi-Fi technology.
2) It supports a high data rate, up to 100 Mbps at long ranges up to 50 km.
3) Easy addition of new sectors allows operators to scale the network as the customer base grows, i.e. the scalable system capacity.

4) Advanced techniques (mesh, beam-forming, MIMO) improve non-line-of-sight performance.

5) It supports the Quality of Service that is not fully supported by IEEE 802.11.

Since a WLAN telemedicine system can access the Internet via WiMAX according to the 802.16a, the medical data could be transmitted beyond the limit range of the WLAN to a greater distance. The equivalent high data rate maintains the healthcare services that are available on the WLAN. The fast development of WiMAX allows the deployment of telemedicine, saving more and more people during emergencies.

References

[1] A. H. Association, "New Stats Show Heart Disease Still America's No.1 Killer, Stroke No.3", Jan 2004, http://www.americanheart.org/presenter.jhtml?identifier=3018015, (Access in: Mar 2004)

[2] A. H. Association, "Heart Disease and Stroke Statistics - 2005 Update", 1st Jan, 2005, http://www.americanheart.org/presenter.jhtml?identifier=1928, (Access in: Feb 2005)

[3] C. Gorman, "Why so Many Are Getting Diabetes", *TIME,* vol.163, No.2, pp.44-49, 12 Jan 2004.

[4] R. S. H. Istepanian, *et al.*, "m-Health: Beyond Seamless Mobility and Global Wireless Healthcare Connectivity", *IEEE Transactions on Information Technology in Biomedicine,* vol.8, No.4, pp.405-414, Dec. 2004.

[5] H. Lamminen, *et al.*, "A Three-year Follow-up of Finnish Telemedicine Programmes", *IEEE Transactions on Information Technology in Biomedicine,* vol.5, No.2, pp.174-177, Jun 2001.

[6] J. C. Lin, "Applying Telecommunication Technology to Health-Care Delivery: The Current Status and Challenges of Telemedicine", *IEEE Engineering in Medicine and Biology,* pp.28-31, Jul/Aug 1999.

[7] C. S. Pattichis, *et al.*, "Wireless Telemedicine Systems: An Overview",

IEEE Antenna's and Propagation Magazine, vol.44, No.2, pp.143-153, Apr 2002.

[8] B. Woodward, *et al.*, "The Use of Mobile Telephone Networks and Wireless Internet Technology for Monitoring Patients Remotely", presented at *3rd Seminar on Appropriate Medical Technology for Developing Countries*: The IEE, London UK, 4th Feb 2004.

[9] C.-C. Lin, *et al.*, "A Unified Multimedia Database System to Support Telemedicine", *IEEE Transactions on Information Technology in Biomedicine,* vol.2, No.3, pp.183-192, Sep 1998.

[10] A. I. Hernandez, "Real-Time ECG Transmission Via Internet for Nonclinical Applications", *IEEE Transactions on Information Technology in Biomedicine,* vol.5, No.3, pp.253-257, Sep 2003.

[11] U. Engelmann, *et al.*, "A Three-Generation Model for Teleradiology", *IEEE Transactions on Biomedical Engineering,* vol.2, No.1, pp.20-25, Mar 1998.

[12] A. P. Anagnostaki, *et al.*, "A Novel Codification Scheme Based on the "VITAL" and "DICOM" Standards for Telemedicine Applications", *IEEE Transaction on Biomedical Engineering,* vol.49, No.12, pp.1399-1411, Dec 2002.

[13] J. Bai, *et al.*, "A Portable ECG and Blood Pressure Telemonitoring System", *IEEE Engineering in Medicine and Biology,* pp.63-70, Jul/Aug 1999.

[14] E. J. Gomez, *et al.*, "A Broadband Multimedia Collaborative System for Advanced Teleradiology and Medical Imaging Diagnosis", *IEEE*

Transactions on Information Technology in Biomedicine, vol.2, No.3, pp.146, Sep 1998.

[15] S. Pavlopoulos, *et al.*, "A Novel Emergency Telemedicine System Based on Wireless Communication Technology --- AMBULANCE", *IEEE Transactions on Information Technology in Biomedicine,* vol.2, No.4, pp.261-267, Dec 1998.

[16] K. Kong, "Web-Based Monitoring of Real-Time ECG Data", *Computers in Cardiology,* pp.189-192, 2000.

[17] L. Pirrucc, *et al.*, "An Interactive Multimedia Satellite Telemedicine Service", *IEEE Multimedia,* pp.76-83, Apr-Jun 2000.

[18] J. Farserotu., "A Survey of Future Broadband Multimedia Satellite system, Issues and Trends", *IEEE Communications Magazine,* pp.128-133, Jun 2000.

[19] F. Beltrame, *et al.*, "Adopting Telemedicine Services in the Airline Framework", *IEEE Transactions on Information Technology and Biology,* vol.5, No.2, pp.171-174, Jun 2001.

[20] C. Kugean, *et al.*, "Design of a Mobile Telemedicine System with Wireless LAN", presented at *Asia-Pacific Conference on Circuit and Systems*, 28-31 Oct. 2002.

[21] K. Banitsas, *et al.*, "Applications of Medical Wireless LAN (MedLAN) Systems", *International Journal of Health Marketing,* vol.2, No.2, pp.136-142, 2002.

[22] M. Li, *et al.*, "3G Network Oriented Mobile Agents for Intelligent

Diabetes Management: a Conceptual Model", presented at *Proc of the 4th Annual IEEE Conf. on Information Technology Applications in Biomedicine*, UK, 2003.

[23] S. Laxminarayan, "Unwired E-Med: the Next Generation of Wireless and Internet Telemedicine Systems", *IEEE Transactions on Information Technology in Biomedicine*, vol.4, No.3, pp.189-192, Sep 2000.

[24] B. Woodward, *et al.*, "Wireless Telemedicine: the Next Step?" presented at *Proc of the 4th Annual IEEE Conf on Information Technology Applications in Biomedicine*, UK, Birmingham, UK, 2003.

[25] B. Woodward, *et al.*, "Design of a Telemedicine System Using a Mobile Telephone", *IEEE Transactions on Information Technology in Biomedicine*, vol.5, No.1, pp.13-15, Mar. 2001.

[26] D. L. Paul, *et al.*, "Assessing Technological Barriers to Telemedicine: Technology-Management Implications", *IEEE Transactions on Engineering Management*, vol.46, No.3, pp.279-288, Aug 1999.

[27] T. S. Rappaport, "Wireless Communications: Principles and Practice (2nd Edition)". ISBN: 00780311671, New Jersey: Prentice Hall PTR, 31 Dec, 2001.

[28] M. Shafi, *et al.*, "Wireless communications in the 21st century". ISBN: 0-471-15041-X: Wiley-IEEE Press, Mar 2002.

[29] J. D. Gibson, "The Mobile Communications Handbook - Second Edition". ISBN: 3540648364, New Jersey, US: Springer-Verlag New York, Inc, 1999.

[30] A. Santamaria, *et al.*, "Wireless LAN Systems". ISBN: 0890066094, London: Artech House, 1994.

[31] W. Allyn, "Understanding the Wireless Medical Band and the Wireless Medical LAN", Welch Allyn Protocol Inc, May 2001, http://www.monitoring.welchallyn.com/pdfs/resourcelib/study_guide.pdf, (Access in: Oct. 2004)

[32] H. Honkasalo, "W-CDMA and WLAN for 3G and Beyond", *IEEE Wireless Communications*, vol.9, No.2, Apr 2002.

[33] G. Legg, "Beyond 3G: The Changing Face of Cellular", Apr. 21, 2005, http://www.techonline.com/community/tech_topic/37977, (Access in: Oct. 2005)

[34] W. Carney, "IEEE 802.11g New Draft Standard Clarifies Future of Wireless LAN", Texas Instrument Incorporated, 2002, http://focus.ti.com/pdfs/bcg/802.11g_whitepaper.pdf, (Access in: Oct. 2005)

[35] B. Corporation, "IEEE 802.11g: The New Mainstream Wireless LAN Standard", Broadcom Corporation, 2003, http://www.broadcom.com/collateral/wp/802.11g-WP104-R.pdf, (Access in: Oct. 2005)

[36] I. D. Drivers, "Introduction to IEEE 802.11", http://www.intelligraphics.com/articles/80211_article.html, (Access in: Oct. 2005)

[37] W. R. Stevens, "TCP/IP Illustrated Series", vol.1: Protocols, 1994.

[38] C. J. Mitchell, "Security for Mobility". ISBN: 0863413374, Herts, UK: Institution of Electrical Engineers, 2003.

[39] R. D. Vines, "Wireless Security Essentials: Defending Mobile Systems from Data Piracy". ISBN: 0-471-20936-8, Indianapolis, Indiana: Wiley Publishing, Inc., 2002.

[40] D. Halasz, "IEEE 802.11I and Wireless Security", 2004, Http://www.embedded.com/showArticle.jhtml?articleID=34400002, (Access in: Oct. 2004)

[41] M. W. Oliphant, "The Mobile Phone Meets the Internet", *IEEE Spectrum*, pp.20-28, Aug 1999.

[42] L. Biel, "ECG Analysis - a New Approach in Human Identification", *IEEE Transactions on Instrumentation and Measurement*, vol.50, No.3, pp.808-812, Jun 2001.

[43] J. Yang, "Modern Electrocardiography". ISBN: 7030060008/R.307, Beijing: Science and Technology Publishing House, 1997.

[44] W. Stallings, "Cryptography and Network Security: Principles and Practice (3rd Edition)". ISBN: 0130914290: Prentice Hall, Aug 27, 2002.

[45] K. Sayood, "Lossless Compression Handbook". ISBN: 0126208611, London: Academic Press, 2003.

[46] M. Norman, "Database design manual: using MySQL for Windows". ISBN: 1-85233-716-8, London: Springer Professional Computing, 2004.

[47] K. Kong, *et al.*, "Web-Based Monitoring of Real-Time ECG Data", *Computers in Cardiology*, pp.189-192, 24-27 Sep. 2000.

[48] C. Lau, *et al.*, "Asynchronous Web-Based Patient-Centered Home Telemedicine System", *IEEE Transactions on Biomedical Engineering,* vol.49, No.12, pp.1452-1462, Dec. 2002.

[49] C. J. Mitchell, "Security for Mobility". ISBN: 0863413374, Stevenage, Herts, UK: Institution of Electrical Engineers, 2003.

[50] G. M. Koien, *et al.*, "Security aspects of 3G-WLAN interworking", *Communications Magazine, IEEE,* vol.41, No.11, pp.82 - 88, Nov. 2003.

[51] W. Forum, "WiMAX Forum Overview", WiMAX Forum, http://www.wimaxforum.org/about/, (Access in: Oct. 2005)

[52] W. Forum, "IEEE 802.16a Standard and WiMAX Igniting Broadband Wireless Access", WiMAX Forum, 06/01/04, http://www.wimaxforum.org/news/downloads/WiMAXWhitepaper.pdf, (Access in: Oct. 2005)

[53] G. Antonello, *et al.*, "WiMAX - General Session", WiMAX Forum, 20 Jan, 2004, http://www.wimaxforum.org/news/events/wimax_day_agenda/WiMAX_-_General_Session_TWG.pdf, (Access in: Oct. 2005)

APPENDIX

A1 Software Design

A1.1 The Remote Interface

(a) A doctor logs into a given database server using his unique user ID and password. **Figure A.1** is the login window.

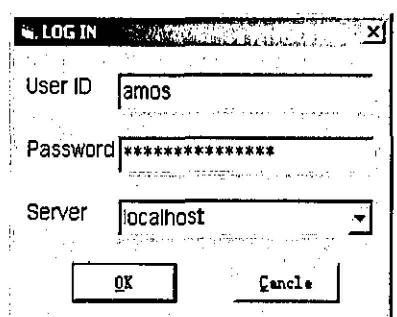


Figure A. 1 The Log-in window in RI

(b) If he passes the identification, the main window for patients' information follows, as described in **Figure A.2**.

- The tree-list on the left shows all the databases and tables that the doctor is allowed to access (both to read and to write). The doctor is allowed to access three databases of "MySQL", "telemedicine", and "test".

- The list on the right contains the main content of the table chosen in the tree-list. For example, when he chooses the table "patient" in telemedicine, all his patients are listed, ordered by name, with three pieces of basic information of "Name", "Sex" and "Birthday".

- The doctor can sort the content into different orders by clicking the column-headers.

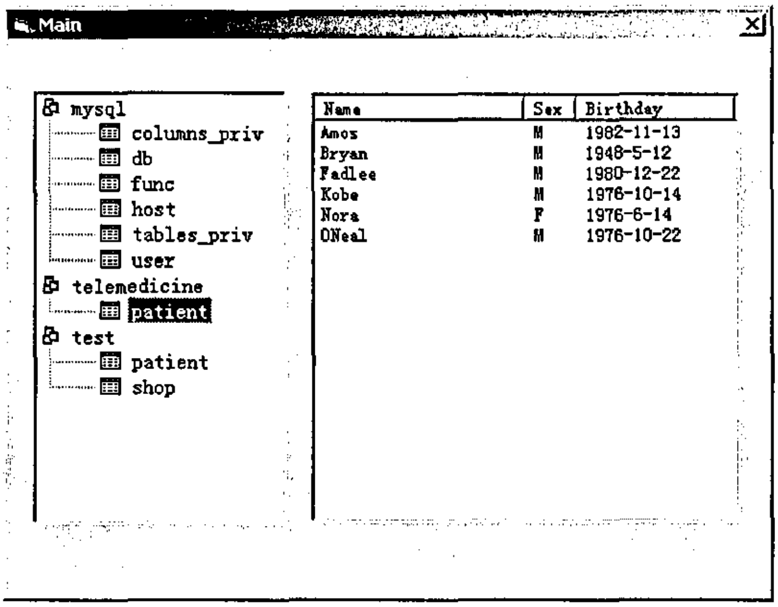


Figure A. 2 The main window for patient information in the RI

(c) The doctor double clicks a patient's name, to obtain the detailed information on that patient, which can be seen in **Figure A.3**.

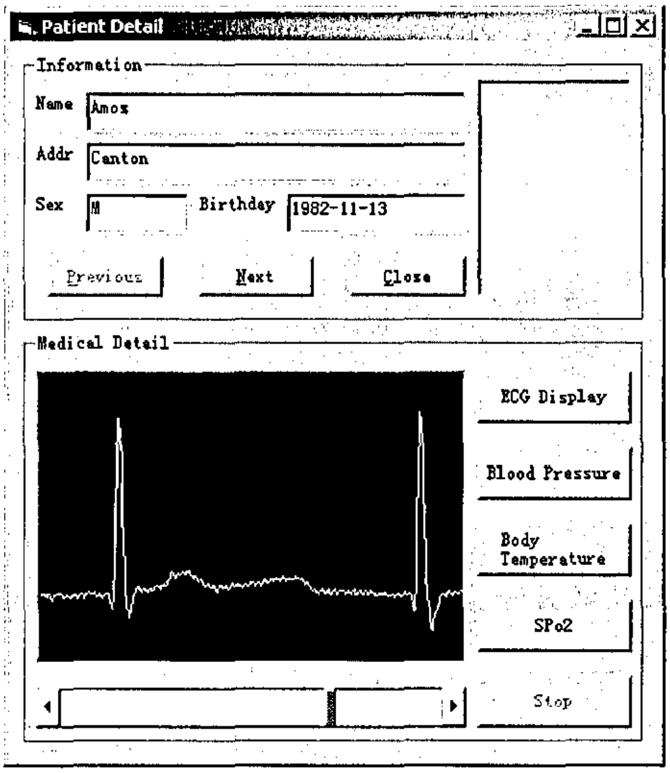


Figure A. 3 The window for patient's detail information in the RI

This window splits into 2 parts.

- The upper part of basic information including name, address, sex, birthday, and a piece of recent portrait.

- The lower part of medical information, including a rolling ECG image, blood pressure, body temperature, and the SpO_2 image. At present only the ECG image is available.

At the moment, only the table "patient" in the database "telemedicine" is extendable.

A1.2 The Multi-User Local Interface

The LI (**Figure A.4**) is able to deal with more than one patient data packets at a time, and the maximum number (2 at the moment) is set by the DBA. In case of more users, a maximum number of users are served, and the rest waits. When it receives a valid data packet, it interprets the packet into corresponding cells and meanwhile loads them into the database. At present, the "Name" here is temporarily treated as the 16-byte ID in the data packet.

However, as mentioned before, all these operations are supposed to be transparent. And thus, this programme is not the real software working in the final system, but conceptually telling how the LI works as a "server" in the network part of the telemedicine system, whereas the mobile patient module works as a "client".

A1.3 A Simulation of the Mobile Patient Module

A software programme (**Figure A.5**) simulates the mobile patient module (hardware). It is run on a computer holding a fixed IP address, which is set to be the destination IP in the mobile patient module part. It is uncontrollable and works automatically. It combines different medical signals into a data packet and sends the packet to the LI, working in the same way as the hardware does.

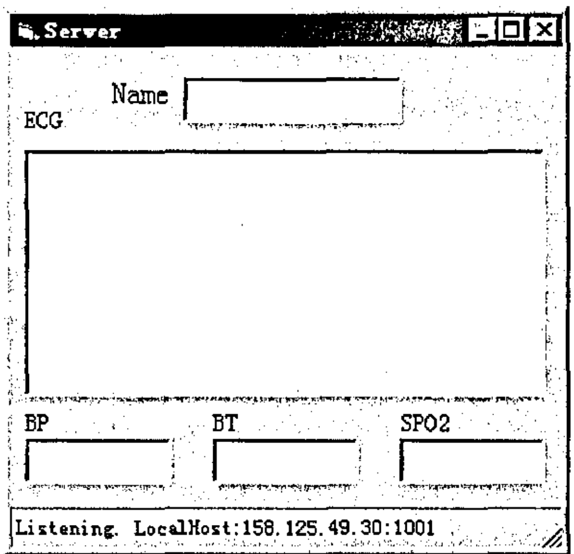


Figure A. 4 The LI window

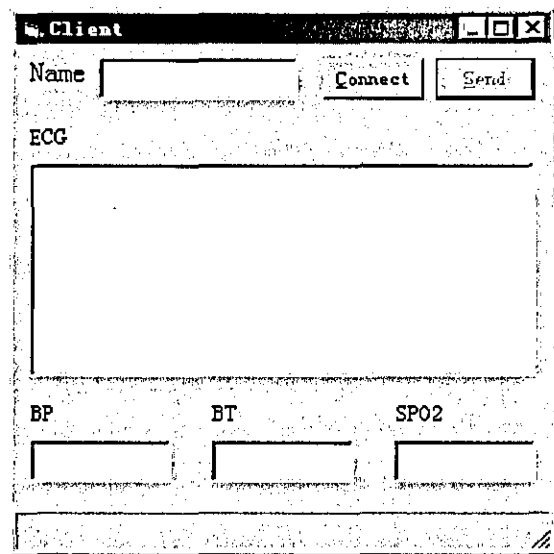


Figure A. 5 The simulation software of the mobile patient module as clients

A1.4 Communication Protocol

Since the LI could only serve a limited number of users, the mobile module should cope with the LI in sending data. We established a waiting protocol to optimise the data transmission over the Internet.

a) The LI listens to the network for new connection requests.

b) The mobile patient module sends a connection request to the LI.

c) The LI checks the number of users being served for free threads. If any, the LI accepts the request; otherwise the LI puts the request into the waiting list.

d) An old user closes his connection and the LI releases the thread.

e) The LI accepts a request on the waiting list and assigns the thread to the relevant user and thus a connection is established.

f) In practice, in order to decrease the probability of user conflict and to shorten the waiting time, we designate that once a user finishes sending his data packet, the LI closes his connection immediately.

However, it is unreasonable for a user to wait endlessly, which hinders the mobile patient module's function. To eliminate this case, we put forward a Resend scheme. Once the mobile patient module waits for too long a period, it stops connecting and retries later. The time interval can be either random or fixed. Further research is needed on this problem. **Figure A.6** gives an example of the protocol processing in detail.

Time slot	**Local Interfacing**	$User_1$	......	$User_k$	......	$User_{max}$	$User_{max+1}$
1	**(a)** Listening	Being served	Being served	Being served	Being served	Being served	**(b)** Sends a connection request
2	**(c)** Checks for free threads						Waiting to be accepted
3	**(c)** Keeps the *request*$_{max+1}$ waiting						
4	Listening						
5				**(d)** Connection Closed			
6	**(d)** Releases thread **k**						
7	**(e)** Accepts the *request*$_{max+1}$ and assigns it to thread **k**						**(e)** Connection established
8	Listening						Being served ......
9							

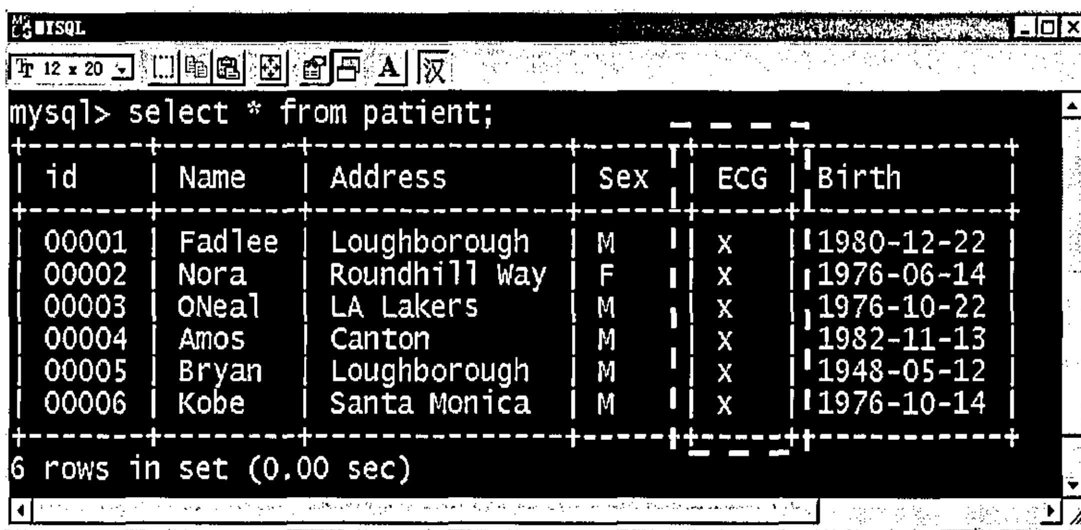
Figure A. 6 An example of the protocol process

A2A Test of the LI in A Multi-user Case

It is to test whether the LI could work properly in a multi-user case.

A2.1 Preliminary work

Before running the LI programme, we set the maximum user number as two. Checking the database, we can see that the ECG records of patients are all "**x**" (an initialised value before a real record comes, **Figure A.7**).

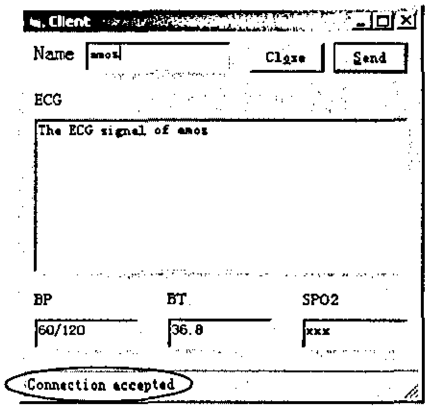


```
mysql> select * from patient;
+-------+--------+---------------+-----+-----+------------+
| id    | Name   | Address       | Sex | ECG | Birth      |
+-------+--------+---------------+-----+-----+------------+
| 00001 | Fadlee | Loughborough  | M   | x   | 1980-12-22 |
| 00002 | Nora   | Roundhill Way | F   | x   | 1976-06-14 |
| 00003 | ONeal  | LA Lakers     | M   | x   | 1976-10-22 |
| 00004 | Amos   | Canton        | M   | x   | 1982-11-13 |
| 00005 | Bryan  | Loughborough  | M   | x   | 1948-05-12 |
| 00006 | Kobe   | Santa Monica  | M   | x   | 1976-10-14 |
+-------+--------+---------------+-----+-----+------------+
6 rows in set (0.00 sec)
```

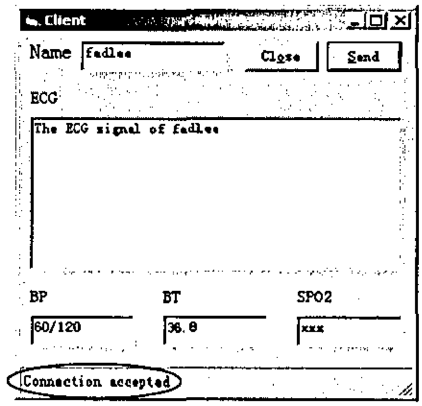
Figure A. 7 The database records before the test

A2.2 In Testing

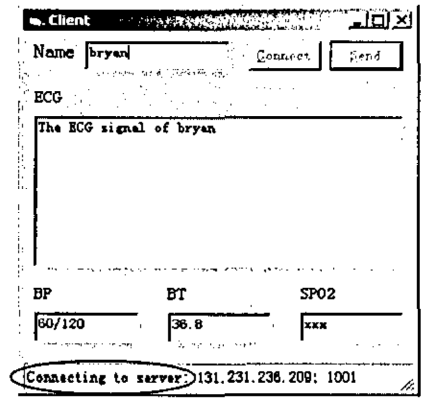
- Firstly, we let the LI is listen to the network, and run four client software at the same time, showing that four different MMs are ready to send their data.
- Secondly, we send four connection requests from these clients (one request from each client, **Figure A.8**). We do not send any data so that no connection is closed when the last request comes.
- Thirdly, then we send a set of data from a client "amos" (**Figure A.9**).
- Finally, we send data from other clients one by one.



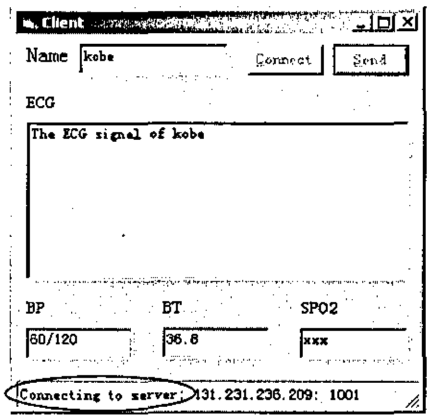
(a) Client amos sets up a connection to the LI



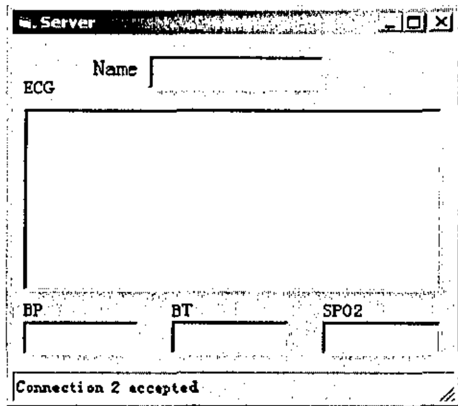
(b) Client fadlee sets up a connection to the LI



(c) Client bryan is waiting to be accepted

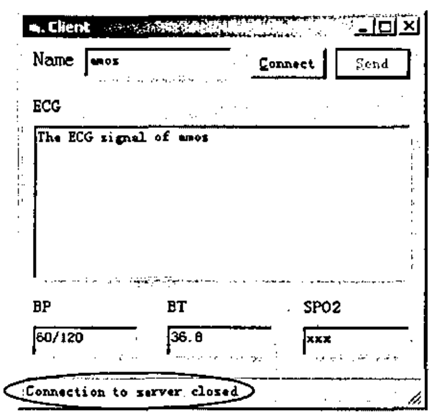


(d) Client kobe is waiting to be accepted

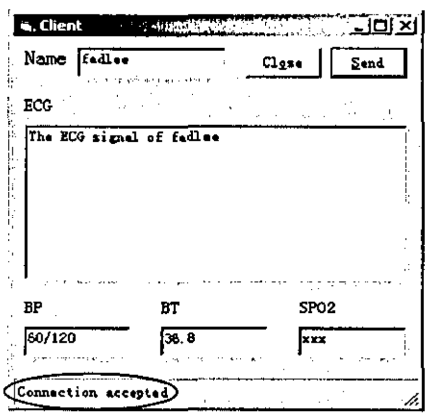


(e) The LI accepts two connections, waiting to receive data

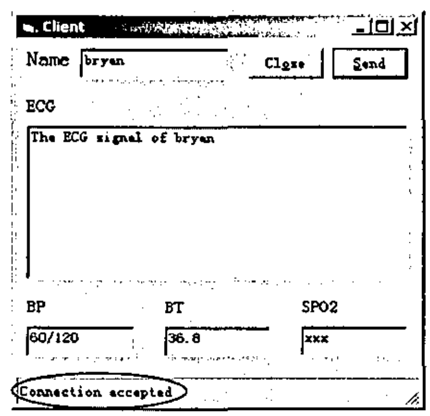
Figure A. 8 Four clients requests when the LI's maximum-thread is two



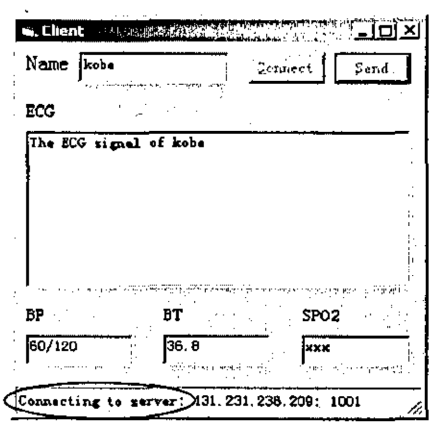
(a) Client amos closes the connection to the LI



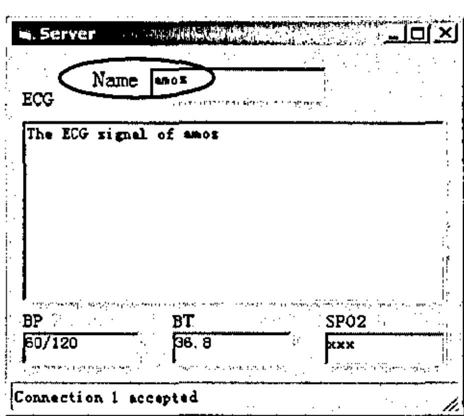
(b) Client fadlee is still connecting to the LI



(c) Client bryan sets up a connection to the LI



(d) Client kobe is still waiting to be accepted



(e) The LI receives the data from client amos

Figure A. 9 Sending data from a client "amos"

A2.3 Result

- Firstly in **Figure A.8**, four connection requests at a time, two are accepted (a and b), and two are waiting (c and d).

- Secondly in **Figure A.9**, client "amos" finishes sending data and the LI extracts the data packet and closes his connection (a). A waiting request "bryan" is then accepted immediately (c). An old client "fadlee" is still being served (b) and another request "kobe" is still waiting (d).

- Thirdly, when we take a look at the database, we find that the ECG record of patient "amos" has changed into "The ECG signal of amos", which is within the packet sent by the client "amos" (**Figure A.10**).

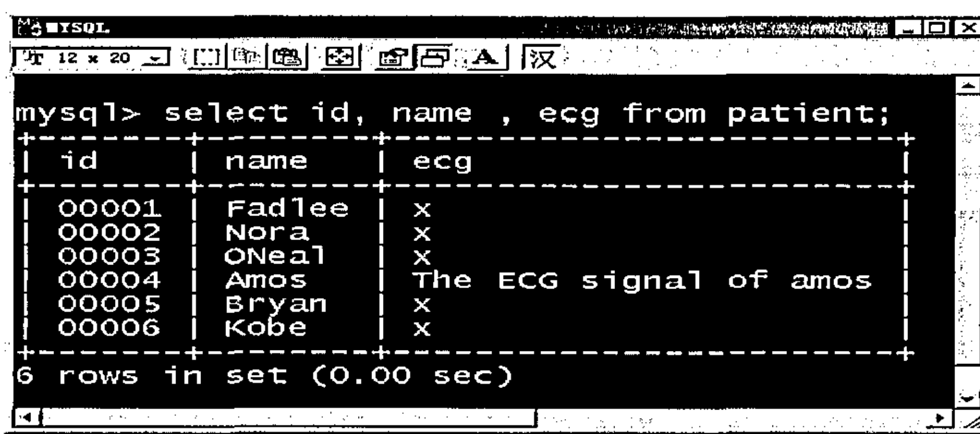
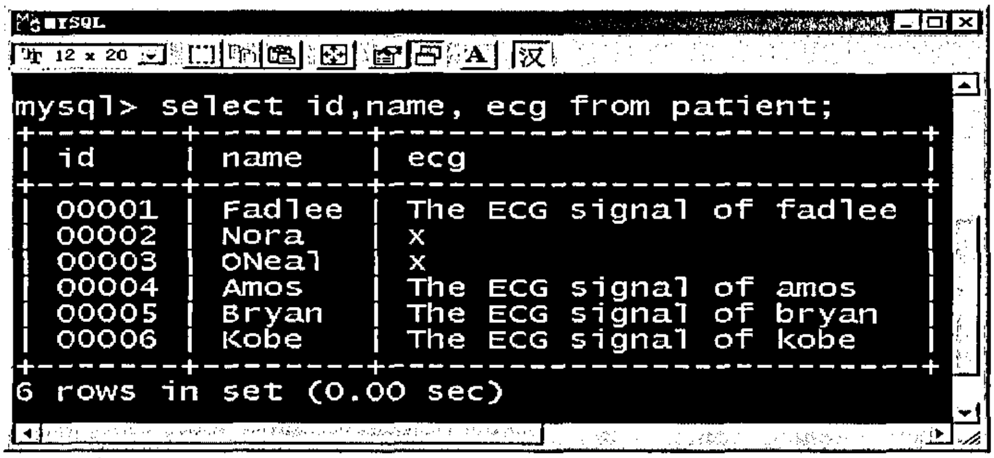


Figure A. 10 The ECG records in the database after client "amos" sent his data

- Finally, after all client finish sending their data, their relevant ECG records have been changed into a same format as amos's (**Figure A.11**).

A2.4 Conclusion

In the test, the LI is able to serve a maximum number of clients, and keep scanning free threads for waiting clients. That means, it works in exactly the right way, which indicates that the LI can handle the over-maximum user case correctly.



```
mysql> select id,name, ecg from patient;
+-------+--------+---------------------------+
| id    | name   | ecg                       |
+-------+--------+---------------------------+
| 00001 | Fadlee | The ECG signal of fadlee  |
| 00002 | Nora   | x                         |
| 00003 | ONeal  | x                         |
| 00004 | Amos   | The ECG signal of amos    |
| 00005 | Bryan  | The ECG signal of bryan   |
| 00006 | Kobe   | The ECG signal of kobe    |
+-------+--------+---------------------------+
6 rows in set (0.00 sec)
```

Figure A. 11 The ECG records in the database after all four clients sent their data