Wireless telemedicine and m-health: technologies, applications and research issues

Yang Xiao*, Daisuke Takahashi and Jing Liu

Department of Computer Science,
The University of Alabama,
Tuscaloosa, AL 35487, USA
Email: yangxiao@ieee.org
Email: daisuke332003@yahoo.com
Email: jliu39@crimson.ua.edu
*Corresponding author

Hongmei Deng

Intelligent Automation Inc.,
15400 Calhoun Drive, Suite 400,
Rockville, MD 20855, USA
Email: hdeng@i-a-i.com

Jingyuan Zhang

Department of Computer Science,
The University of Alabama,
Tuscaloosa, AL 35487, USA
Email: zhang@cs.ua.edu

Abstract: Telemedicine is not medicine, but it is used to compute, to communicate and to deliver high-quality medical care regardless of location. It reduces cost, time and resources. Furthermore, wireless technologies play significant roles in telemedicine, and they are therefore called wireless telemedicine or mobile-health. This paper provides a comprehensive survey on wireless telemedicine, including the relevant wireless technologies, applications and research issues.

Keywords: telemedicine; wireless; m-health; e-health; RFID; radio frequency identification; WLAN; wireless local area network; WPAN; wireless personal area network; 3G/4G.

Reference to this paper should be made as follows: Xiao, Y., Takahashi, D., Liu, J., Deng, H. and Zhang, J. (2011) 'Wireless telemedicine and m-health: technologies, applications, and research issues', *Int. J. Sensor Networks*, Vol. 10, No. 4, pp.202–236.

Biographical notes: Yang Xiao is currently at the Department of Computer Science in The University of Alabama. His research areas are security and communications/networks. His research has been supported by the US National Science Foundation (NSF), US Army Research, Global Environment for Network Innovations (GENI), Fleet & Industrial Supply Center San Diego (FISCSD), FIATECH and The University of Alabama's Research Grants Committee.

Daisuke Takahashi is a Software Engineer at the Konica Minolta Systems Laboratory, Inc. He is currently involved in a variety of software products which are related to Multi Function Product (MFP). He earned his BA degree in Philosophy from Chuo University in Japan in 1998 and his MS degree in Computer Science from The University of Alabama in 2008. He is a former Lab Member at W4-Net Lab in the Department of Computer Science in The University of Alabama. As a graduate student, he won Outstanding Research by a Masters Student for the College of Engineering for 2008–2009 at The University of Alabama.

Jing Liu is a PhD student at the Department of Computer Science in The University of Alabama. He received his BSc and MSc degrees from the Hunan University (China) in 2005 and 2008, respectively. He is an Active Researcher in the area of network security, smart grid, bio-inspired network and telemedicine, including botnet issues, visual attention, anonymous communication and accountability in telemedicine.

Hongmei Deng is currently is a Principal Scientist at Intelligent Automation, Inc. (IAI), Maryland. He received her PhD in Electrical Engineering from the University of Cincinnati in 2004, majoring in Communications and Computer Networks. At IAI, she is currently leading a

number of networks and security related projects, such as secure routing in airborne networks, network service for airborne networks, denial of service mitigation, trust management for wireless sensor network, intrusion detection for MANET and acoustic sensor network for structural health monitoring. Her primary research interests include protocol design, analysis and implementation in wireless ad hoc/sensor networks and network security.

Jingyuan Zhang is currently an Associate Professor at the Department of Computer Science in The University of Alabama. He received his PhD degree in Computer Science from Old Dominion University in 1992. Prior to joining The University of Alabama he was a Principal Computer Scientist with ECI Systems and Engineering, an Assistant Professor with Elizabeth City State University and an Instructor at the Ningbo University. His current research interests include wireless networks, mobile computing and collaborative software.

1 Introduction

The recent development in telemedicine is the evolution from conventional desktops to modern wireless systems, called wireless telemedicine or m-health or mobile-health, normally with wearable medical devices and wireless communication networks (Istepanian et al., 2004). As opposed to portable devices, wearable medical devices are developed to collect medical data at any time without disrupting the users' normal daily lives. Previously, they had to visit clinics or hospitals in person for the same purpose. The advancement in wireless communication technology overcomes most geographical, temporal and even organisational barriers to facilitate a completely roaming way of transferring medical data and records (Hung and Zhang, 2003).

On the other hand, telemedicine is a technology that enables doctors to carry out remote diagnoses. Telemedicine began with a closed circuit TV connection between two places that was designed to conduct discussions about each other's patient cases and also to conduct real-time medical examinations of remote patients (Adler, 2000). Besides video conferencing with audio-visual facilities, some recent telemedicine technologies involve multiple biomedical sensors that are put on patients' bodies and send vital signals automatically to a base station at hospitals via the internet.

The primitive telemedicine system can be traced back to 1959, when several audio-visual data transmission experiments were done successfully (Adler, 2000). Since then, a number of new technologies, such as wireless connectivity, image processing and Virtual Reality (VR), have been integrated into the system (Adler, 2000). Accordingly, telemedicine systems have been substantially brought up to date with today's style in the industrialised world. About ten years after the implementation in Nebraska, another telemedicine experiment was carried out. Massachusetts General Hospital (MGH) was linked to Boston Logan airport to perform immediate consultations for airport employees and passengers in radiology, dermatology and cardiology (Bashshur et al., 1975). Furthermore, the National Aeronautics and Space Administration (NASA) also employed telemedicine instrumentation pack for the International Space Station (ISS) (Studer, 1999). Currently, the flexibility of the systems makes telemedicine applicable to mass casualty disasters, such as earthquakes or tsunamis (Shnayder et al., 2005). In mass casualty disasters, the number of victims increases rapidly in a very short time period, and, accordingly, quickly overwhelms the number of emergency medical staff. In such cases, portable telemedicine packages are distributed to every patient, and vital signals are relayed to the Emergency Medical Services (EMS) devices via the distributed sensors in multi-hopping. However, when the systems require more functionality, more sophisticated techniques are required to be applied. For example, CodeBlue of Harvard University utilises the Adaptive Demand-driven Multicast Routing (ADMR) protocol (Shnayder et al., 2005; Chen et al., 2006) to find efficient routes to the destination. Finally, when implanting biomedical sensors into human bodies, the rising temperature of the sensors will damage surrounding tissues. In this case, Thermal Aware Routing Algorithms (TARAs) must be developed.

As we can see, telemedicine technologies are affected by both the progress of information technology (IT) and the progress of medical peripherals. For example, pulse oximeters can sample blood oxygen saturation (SpO_2), heart rate (HR) and plethysmogram waveform in a non-invasive way without any pain. To record these physiological parameters, a patient just puts one of his/her index fingers into a plastic housing with a pulse oximetry recorder. Also, because of the recent progress of the radio sensor devices, integrating motes into biomedical sensors not only enables the sensors to be wirelessly connected but also reduces the whole size of the medical peripherals. Collaboration of this non-invasive medical technique and a wireless network make the telemedicine modules less obtrusive to patients so that they sense the equipments less. This advantage benefits extended vital signal monitoring and is suited for rehabilitations at home.

Along with the development of technologies, related security issues have increased and cannot be ignored. Due to the small variety of messages transacted between the sensors and personal server (PS), a variety of encrypting patterns is required. Although some security protocols are already defined by network standards, those which cannot be are complemented at the application layer.

Although many works exist in the field of wireless telemedicine, there is no good survey paper about this topic. In this paper, we present a survey on wireless telemedicine and m-health. The purpose of this work is partially to stimulate more researches in wireless telemedicine.

The rest of the paper is organised as follows: In Section 2, we give a definition, history and current state of telemedicine in order to capture a high-level view of the system architecture and to cover the standard model of the conventional and wireless telemedicine systems, architecture and scenarios. Section 3 describes the fundamentals of telemedicine architecture. Section 4 provides technologies for wireless telemedicine. Section 5 introduces medical peripherals for telemedicine. We present some telemedicine applications as well as some experiments and current implementations in Section 6. Network research issues including wireless network issues, routing protocols, securities and Quality of Service (QoS) are explored in Section 7. We conclude this paper in Section 8.

2 Telemedicine background

2.1 Definition of telemedicine

Many organisations and papers have been encouraged to define the telemedicine. The authors Bashshur et al. (1997) tried to define telemedicine: "Broadly, telemedicine involves the use of modern information technology, especially two-way interactive audio and video telecommunications, computers and telemetry, to deliver health services to remote patients and to facilitate information exchange between primary care physicians and specialists at some distances from each other". Later, William Darkins defined the word 'telemedicine' as "health care carried out at a distance" (Hackney, 2005). More specifically, the World Health Organization (WHO) defines telemedicine as, "…the practice of medical care using interactive audio-visual and data communications including medical care delivery, diagnosis, consultation and treatment, as well as education and the transfer of medical data" (Adler, 2000). Recently, the areas of telemedicine have expanded to include emergency healthcare, telecardiology, telepathology, teledermatology, teleophthalmology, teleoncology, telepsychiatry, etc.

By keeping these definitions and techniques in mind, telemedicine can be defined as an information technology that enables doctors to perform medical consultations and diagnoses away from patients. That is doctors can remotely examine patients by viewing and asking symptoms via monitors and sound devices and gather physiological data through telecommunication.

2.2 History of telemedicine

An initial model of telemedicine architecture came more than five decades ago. In 1959, medical consultations between the Nebraska Psychiatric Institute and the Norfolk Hospital were experimentally carried out using a closed circuit TV connection (Adler, 2000). Through this communication, doctors on both sides discussed each other's patient cases and diagnosed psychiatric patients (Adler, 2000).

In 1968, a microwave video link was established between MGH and Logan Airport in Boston (Bashshur et al., 1975). Since this medical connection to MGH enabled instant consultations for radiology, dermatology and cardiology to both airport employees and passengers, it reduced the necessity of having doctors permanently stationed at the airport and lessened flight delays due to patient transportations.

NASA also has employed telemedicine instrumentation packs in the ISS since early manned missions (Studer, 1999). These instrumentation packs utilise a suitcase-sized package that includes an endoscope, ophthalmoscope, dermatology macro-imaging lens, electrocardiograph (ECG), automatic blood pressure sensor, electronic stethoscope, pulse oximeter and a computer with a two-way voice and video control, and are designed to monitor astronauts' physiological data and to send them to the ground (Lau, 1998). More challengingly, NASA is exploring the development of expert systems based on artificial intelligence according to which astronauts in space can be supported to make instant medical decisions regardless of the lack of doctors (Adler, 2000).

Moreover, Lau (1998), researchers from Yale University and MIT, developed Everest Extreme Expedition (E3), which was capable of communicating audio-visually from Mount Everest to the base camp, MIT, Yale Medical and Walter Reed Army Hospital via satellite in 1998.

Adler (2000) reported that the MIT Media Laboratory successfully developed prototypes of the low-cost portable telemedicine kit targeting patients in developing countries as part of the Little Intelligent Communities (LINCOS) project. The purpose of the LINCOS project was to deploy not only the telemedicine systems, but also high-speed internet, telecommunications and distant education to rural areas of developing countries where people suffer from a shortage of doctors or medical specialists. Although the prototypes of this portable telemedicine kit consists of a digital stethoscope, ECG recorder, medical imaging system and blood pressure and temperature measurement, it only cost around $8000 (Adler, 2000).

The LINCOS project offered 'digital town centres' to rural regions so that services such as public phones, faxes, internet, distant education and telemedicine could share a common data connection in order to reduce the cost of connectivity (Adler, 2000). Structurally, digital town centres employed revised ISO shipping containers that offer a lot of benefits, such as standardisation, security, structural integrity and low cost, as well as their wide spread transferability, with a tensile structure (Adler, 2000). By using a tensile structure, digital town centres keep the electrical devices from being exposed to outdoor elements (Adler, 2000).

In those areas where neither telephone lines nor high-speed internet connectivity were available, the LINCOS project made use of a Very Small Array Terminal (VSAT), which enabled direct audio-visual data transmission to 'digital town centres' via satellite (Adler, 2000). The VSAT connectivity is purchased from Internet Service Providers (ISP's) cooperating with such companies as Tachyon (based in San Diego, CA), which buys unused bandwidth from existing geostationary satellites and sells it again at reasonable prices (Adler, 2000). Based on Tachyon's website, for example, they were capable of providing around immediate 2 Mbps connectivity for almost all areas

in the USA and Canada, and this connection could be expanded to any place in the world by now (Adler, 2000). In addition, connectivity could be available for nearby schools, offices and houses by placing wired lines to them, or for places several miles away by installing short-range microwave links (operating above 800 MHz) (Adler, 2000). Although existing landlines, if any, are preferable to a satellite link, regular telephone lines (POTS) do not have sufficient capability of data transmission. However, frame relay or DSL would work well (Adler, 2000).

Another application of the telemedicine architecture is to connect the system wirelessly. This telemedicine configuration utilises the wireless LAN or WAN instead of connecting everything with wires in order to enhance the portability of the system (Hackney, 2005). With a wireless telemedicine kit, medical practitioners can make medical consultations directly to patients at home. This type of telemedicine kit benefits the remote real-time healthcare. In addition, since most laptops or tablet PCs now integrate a Wireless Local Area Network (WLAN) module of the IEEE 802.11 standard, wireless telemedicine can be integrated into standard PC systems. According to the studies of telemedicine implementation conducted by the University of Virginia research group, the IEEE 802.11 standard was capable of a video conferencing system, such as the NetMeeting from Microsoft with the H.263 format that utilised the G.723.1 codec for the audio data and CIF, Quarter-CIF (QCIF) and Sub-QCIF for the video (Hackney, 2005).

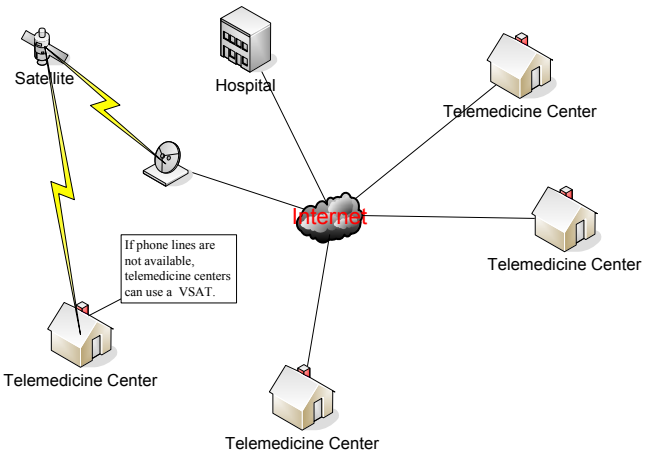
Moreover, recent progress of the sensor technology has enabled miniature, lightweight, low-power, low-cost motes or smart dusts to be commercially available. The miniature motes have the basic functionality of sensing, processing, transmitting and receiving data. Recently, these miniature motes have been integrated into several medical sensors, such as pulse oximeters, ECGs and motion sensors. These sensors are called wearable medical sensors. The wearable medical sensors look like a wearable patch, bandage or a pair of shoes, while they continuously collect patients' physiological data in real time in non-invasive ways (Bonato, 2003; Jovanov et al., 2005). The wearable medical sensors are often accompanied with handheld devices, such as PDAs or tablet PCs, to establish wearable wireless body area networks (WWBANs) around patients. Since the wearable medical sensors can allow patients to be monitored over a long period of time, they are mainly used for ambulatory monitoring, remote monitoring for physical rehabilitations or continuous ECG telemetry (Shnayder et al., 2005). Furthermore, the Harvard University research group is currently exploring the application of these wearable sensors to mass casualty disasters (Shnayder et al., 2005).

2.3 Telemedicine architecture

From the aforementioned definitions and history, in the telemedicine architecture, places where doctors actually carry out medical consultations and where patients receive them are physically different. That is places where doctors will perform medical consultations are mainly hospitals or clinics, while places where patients will be given their medical consultations are places other than hospitals or clinics but facilities which are prepared for the usage of the telemedicine system. These telemedicine facilities should be dispersed around areas evenly so that they can reduce the burden of travelling to hospitals (Hackney, 2005). From the telemedicine facilities, images, videos and physiological data are sent to base stations at hospitals. The data transfers basically utilise the internet through existing phone lines (Adler, 2000). In addition, even though phone lines are not available due to economic conditions in developing countries, some telemedicine facilities can have the ability to establish the internet connection via satellite (Adler, 2000).

The LINCOS project deployed telemedicine facilities, called telemedicine centres, to rural areas of the Dominican Republic and Costa Rica (Adler, 2000). Each telemedicine centre is a small private space which equips an examination table, a mobile sink, a desk and a cabinet for storing medical devices and supplies, and the telemedicine kits are only opened within the telemedicine centres (Adler, 2000). Audio-visual and physiological signals will be captured at the telemedicine centres and sent to nearby hospitals using the internet through existing phone lines. Even if phone lines were not available, a telemedicine centre could establish the internet connection over the VSAT, which enables direct audio-visual data transmission by using a satellite connection, as shown in Figure 1 (Adler, 2000).

Figure 1 A model of telemedicine of LINCOS project (see online version for colours)



3 Wireless technologies

Wireless technologies have already made great impacts on telemedicine. Some of these wireless networks operate at unlicensed frequencies so that they are better protected. Some are applied in ubiquitous network for supporting healthcare services. In this section, we review some wireless technologies that can be used in telemedicine.

3.1 Wireless local area networks

The IEEE 802.11 WLANs (IEEE, 1999) can be major components in telemedicine systems. They operate in Industrial, Scientific and Medical (ISM) bands with several different physical layers. IEEE 802.11b operates in the 2.4 GHz band and has data rates up to 11 Mb/s, whereas IEEE

802.11g, based on Orthogonal Frequency Division Multiplexing (OFDM), operates in the same band and has data rates up to 54 Mb/s. The IEEE 802.11a based on OFDM has data rates of up to 54 Mb/s, but operates in the 5 GHz band. The current IEEE 802.11 specification supports two different mechanisms at the Medium Access Control (MAC) layer: Distributed Coordination Function (DCF) and optional Point Coordination Function (PCF). The DCF is based on Carrier Sense Multiple Access with a Collision Avoidance (CSMA/CA) mechanism, in which a wireless station senses the channel before transmitting a frame. It defines a basic access mechanism and an optional Request-To-Send/Clear-To-Send (RTS/CTS) mechanism. The PCF is an optional, centrally controlled channel access function that provides contention-free (CF) frame transfer. It is designed to support time-bounded services, which can provide limited QoS. Logically, it sits on top of the DCF and performs polling, which enables polled stations to transmit without contending for the channel. It attains a higher priority than the DCF by adopting a shorter Interframe Space (IFS) called the Point Interframe Space (PIFS).

IEEE 802.11e (Xiao and Li, 2004) provides a channel access function called Hybrid Coordination Function (HCF) to support applications with QoS requirements. The HCF includes both contention-based channel access and centrally controlled channel access schemes. The contention-based channel access of the HCF is also referred to as Enhanced Distributed Coordination Function (EDCA).

The current IEEE 802.11 WLANs can be used in wireless telemedicine. IEEE 802.11e can be used for transmitting sensitive medical data with QoS support, and IEEE 802.11i provides security support (Xiao et al., 2006a; Xiao et al., 2007a; Olteanu and Xiao, 2010).

3.2 Wireless personal area networks

Wireless Personal Area Networks (WPANs), such as Bluetooth based on IEEE 802.15.1, have been used in the past for telemedicine. An example of an application of Bluetooth has been reported by Liszka et al. (2004a), where it was used to transmit ECG monitoring data between wearable sensors and a local server in the user's PDA. A piconet is a short-range network supporting up to eight Bluetooth devices to communicate in a peer-to-peer fashion. In a piconet, medium access is controlled by a master device, which allocates time slots for transmissions of the remaining devices. Multiple piconets can be interconnected to form scatternets. Bluetooth operates in the 2.4 GHz ISM band and uses Frequency Hopping Spread Spectrum (FHSS) technology at the physical layer to provide data rates of up to 1 Mb/s.

3.3 4G technology

Users demand seamless switching from one network to another in a telemedicine system. This can be achieved via 4G technologies, which will integrate all networks via IP-based protocol and improve data transfer. 4G networks have some common characteristics as follows: (a) all IP based on network architecture; (b) higher bandwidth and data throughput; (c) integration of heterogeneous access networks; (d) support for multimedia applications.

Future integrated networking scenarios are identified where WLAN and WPAN technologies, operating in unlicensed frequency bands, provide a network infrastructure shared by medical applications with different requirements, as well as by typical IT applications. Due to the life critical nature of some medical applications, the solutions to these challenges to enable such integrated and shared network are not trivial.

3.4 RFID

Radio Frequency Identification (RFID) systems can identify an object or a person by using wireless transmission (Xiao et al., 2006b; Xiao et al., 2007b). An RFID system consists of RFID tags (also called transponders) and readers (also called interrogators). Readers broadcast queries about information contained in tags to tags in their wireless transmission ranges, and tags reply with the requested information such as identification (ID) numbers. Each tag includes a serial number, model number, colour, place of assembly or other data (Xiao et al., 2006b). Tags that do not contain microchips are called chipless tags. On the other hand, tags containing microchips are called chip tags. There are two types of tags: active and passive. An active tag contains a small power source (e.g. a battery), whereas a passive tag does not contain any power source and uses the power generated by a reader. Due to the cost efficiency of mass production of passive tags, most tags are passive. Readers are devices that read/interrogate tags, and each reader is equipped with antennas, a transceiver and a processor. Operating frequency determines the capability of an RFID system, and the Federal Communications Commission (FCC) defines four different frequencies: low frequency at 125 Hz, high frequency at 13.56 MHz, ultra high frequency at 868–915 MHz and microwave at 2.45–5.8 GHz.

Wireless microsensor technology provides a unique opportunity for delivering quality healthcare to patients inside and outside of hospitals. Intel's Caregiver's Assistant and Georgia Tech's Memory Mirror use RFID tags to monitor the activities of the elderly at home and help caregivers improve the quality of healthcare (Baard, 2004; Intel, 2004). In addition to in-home monitoring, RFID tags can be used to monitor patients in a hospital, in an ambulance and even in a disaster area (Hu and Kumar, 2003; Hu et al., 2006b). Hu et al. (2009a) designed a wearable medication monitoring platform that hosts an RFID reader and is capable of radio frequency communication. Thanks to this device, the patient will be able to scan any of their medication bottles containing an RFID tag and wirelessly transmit the attempted drug application to a central workstation for further instruction.

To reduce operating costs, many hospitals adopt an automated inventory control system, and RFID has been the prominent technology to enable asset management.

However, a separate network is needed to operate an RFID-based asset management system and therefore increases the cost. Recently, there has been some interest in WLAN-based technology solutions for this application.

3.5 Mote

The word 'mote' is derived from the word 'remote', and it is merely a miniature wireless transceiver (Webopedia, 2010). Regardless of its miniature size, it can sense, sample and process data like other larger wireless transceivers. Previously, the UC Berkeley and Intel research group designed a low-power, wireless mote, called the MICA mote. This brings its palm size together with basic functionality. The MICA mote can embed an 8 bit microcontroller, 40 kbps radio and local storage performing low battery consumption, which keeps two AA batteries lifetime for 5–6 days if continuously working but saves it for over 20 years in non-active state. The MICA also can employ a 433 or 916 MHz radio whose maximum bandwidth is 76.8 kbps with a 100 m transmission range (Welsh et al., 2003; Malan et al., 2004; Welsh et al., 2004; Welsh, 2005). Likewise, the Harvard University research group developed a tiny prototype mote named Pluto (Malan et al., 2004). Although when compared to the MICA mote the Pluto mote sacrifices expandability and battery durability, it is lighter and smaller than the MICA mote. The Pluto mote can be housed in 57 × 36 × 16 mm OEM plastic enclosure and weigh only 30.5 g. A tiny rechargeable lithium polymer battery powers the mote for around 5 hours.

The miniature motes generally integrate an on-board bio-amplifier, which can be connected to an electromyography (EMG) or an ECG sensor and amplify patients' vital signals so that medical practitioners can electrically observe them on the display of the local main station (Jovanov et al., 2005). In addition, since some applications can integrate accelerometers into a mote, practitioners can monitor human movement from all three dimensional axes, and the feature can be used for computer-assisted physical rehabilitations (Jovanov et al., 2005). However, wireless transmissions have an error rate many times that of a traditional wired network. While there is a need to decrease the one-on-one time staff must spend with each patient, it must be done safely. A loss of medical data typical of that seen in mote transmissions cannot be tolerated because each piece of cardiac data could carry important medical information. To achieve more reliable mote transmissions, Hu et al. (2009a) adopted extended Kalman filter for wireless error recovery in real ECG signals.

4 Wireless telemedicine

Conventional telemedicine systems are designed to be used at particular facilities and can rarely be moved to other places. Therefore, it is not crucial whether they are connected to phone lines or other wired devices. However, telemedicine systems will be of more benefit if they effectively employ portability and are easily carried to patients rather than being fixed at a particular place. Since recent wireless network technology has allowed people to access audio-visual data with handheld devices and, moreover, some companies even offer high-speed data transmissions via smaller antennae over low-orbit satellites, the wireless networks are easily applied to telemedicine technology (Adler, 2000).

Because the main objective of the wireless telemedicine kits is to allow medical practitioners to carry them to patients' homes and set them up there, they are inevitably more compact and simpler than conventional telemedicine systems. This causes the wireless telemedicine kits to sacrifice some of the medical capabilities employed by conventional systems (Hackney, 2005). However, because wireless telemedicine is often applied only to minor medical consultations or specialised healthcares, such as emergency first aid or telecardiology, it is not required to equip all of the features of conventional systems. To the contrary, the conventional telemedicine systems often offer surplus system functionalities for wireless telemedicine.

4.1 Wireless telemedicine architecture

In the context of wireless telemedicine, two portions of the wired connections of the conventional telemedicine systems will be replaced by the wireless network connectivity: one is a connection between the local base station which will aggregate patients' vital data from several medical peripherals locally, and existing phone lines (Hackney, 2005); the other is a connection between the local base station and medical peripherals that establishes the WWBAN (Jovanov et al., 2005; Milenković et al., 2006).

By utilising these two wireless connections, it becomes possible to exploit two types of wireless configurations. The first is to employ the wireless connectivity in only the former part of the connection, i.e. between the local base station of the telemedicine kit and existing phone lines, as shown in Figure 2. In this configuration, the portability of telemedicine kits will be enhanced to allow medical practitioners to carry them to patients' homes and make medical consultations away from the telemedicine facilities. Since this wireless communication will be made up by the WLANs, e.g. the IEEE 802.11 standard, the wireless access points are required to be within the range of the radio transmission. Alternatively, this wireless connection is replaced by a Wireless Wide Area Network (WWAN), such as Ripwave (provided by Navini Networks) (Hackney, 2005). In this case, extra wireless network units, e.g. a modem or a particular PC card, are required to establish the WWAN connectivity. There also need to be companies to offer the WWAN connectivity.

The other configuration is to allow the wireless telemedicine kits to involve both of the aforementioned wireless connections, i.e. between the local base station and medical peripherals as well as a wireless connection between the local base station and existing phone lines, as shown in Figure 3 (Jovanov et al., 2005; Milenković et al., 2006). In this configuration, since patients are comparatively free from the wires connected to the local

main station when within range of the radio transmission, they can easily move around without disturbing the data sampling. The WWBAN connectivity will be established by the IEEE 802.15.1 or IEEE 802.15.4 (10BLADE, 2004; Malan et al., 2004; Gao et al., 2005; Jovanov et al., 2005; Shnayder et al., 2005; Gaynor et al., 2006; Milenković et al., 2006; Te'eni et al., 2007). The wireless transmission ranges will be shorter than those of the WLAN.

Figure 2 Wireless telemedicine system architecture (see online version for colours)

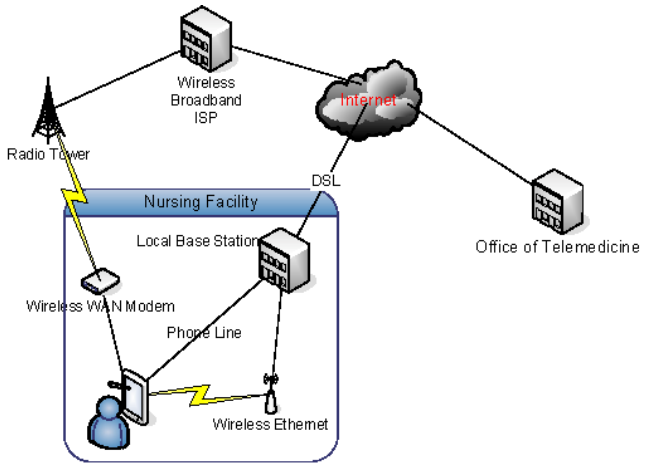
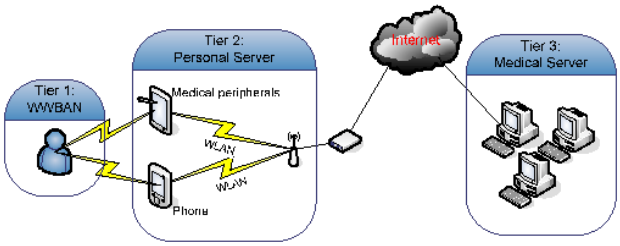


Figure 3 Wireless telemedicine with WWBAN (see online version for colours)

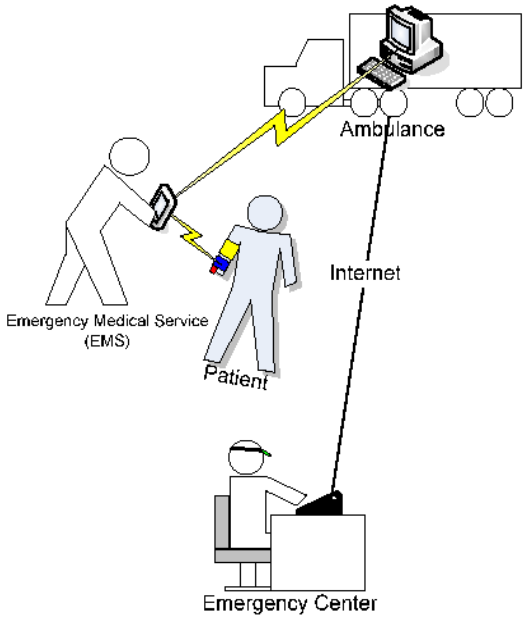


4.2 Wearable medical sensors in WWBAN

The recent progress of sensor technology enables miniature, lightweight, low-power, low-cost wireless transceivers or motes, to be commercially available. The motes have the basic functionality of sensing, processing, transmitting and receiving data, and typically are used for the vehicle tracking or habitat monitoring of ducks (Welsh et al., 2004). However, these miniature transceivers are now ready to be used in medical applications by being integrated into several medical devices.

The wearable medical sensors are built in a wearable patch, bandage or pair of shoes that integrate a mote and a variety of medical sensors collecting patients' physiological data in real time (Bonato, 2003; Jovanov et al., 2005). They can establish the WWBAN around patients. The goal of the wearable medical sensors is to accomplish non-obtrusiveness of the medical sensors in patients. So, even though patients wear a couple of medical sensors for an extended time period, they will have little feeling that they are wearing such medical devices. Also, this non-obtrusiveness will gain freedom of mobility of patients during the medical data collections. Figure 4 shows an example of medical treatments in the emergency case (Gao et al., 2005). This wireless telemedicine application is designed to support patient monitoring, patient record generation and remote patient record review for emergency cases and mass casualty disasters.

Figure 4 Patient information flow (see online version for colours)



During emergency cases, EMS crews will distribute medical care kits with several wearable medical sensors and a mote with a wrist strap to each patient. A mote will be wrapped about the patient's wrist, and medical sensors will be placed on appropriate parts of the patients. Medical sensors will record the patient's physiological data in real time and automatically transmit them to the local base station, e.g. a laptop PC or PDA, which runs the PS occupied by the EMS crew (Gao et al., 2005).

The WWBAN architecture is basically broken down into three tiers, as shown in Figure 3 (Milenković et al., 2006). It mainly consists of the sensing tier, the Graphical User Interface (GUI) and Data Processing (DP) tier, and the database (DB) tier (Gaynor et al., 2007).

4.2.1 Tier one: wearable physiological sensors

The first tier is mainly responsible for sampling the patient's vital signals. This tier includes wearable medical sensors, such as a wearable pulse oximeter, ECG sensor and blood pressure sensor (Milenković et al., 2006). These vital sensors that are integrated with a mote continuously monitor the patient's physiological signals and transmit them in real time to the local client devices, such as PDAs, which are integrated with the receiving mote. Basically, the local client devices are locally used by the medical practitioners. In addition, these wearable sensors have on-board memory so that one practitioner will temporally store the Patient Care Records (PCRs) and another practitioner will load these records when taking over the patient (Gao et al., 2005).

4.2.2 Tier two: personal server running on intermediate terminals

The second tier mainly interfaces with several medical sensors in tier one and the medical personnel. It is also responsible for data communications with the medical server or base station and the database at the hospital. A goal of tier two is to achieve the aggregation of data from the medical sensors, human manual input, flexible user interface configuration and rule-based user input (Gaynor et al., 2007). Tier two usually deploys a variety of local client devices, such as PDAs and tablet PCs, which run the PS that is designed to achieve the aforementioned prospects and has a user-friendly interface that will transact physiological signals and communicate with the medical server (the base station). Usually the data transmission between physiological sensors and the client devices relies on the short-range wireless local network connectivity, such as IEEE 802.15.1 and IEEE 802.15.4, and this connectivity establishes the WWBAN around patients (Chen et al., 2006).

The PS usually provides the audio and user-friendly GUI that helps manual inputs of clinical data and gives early alerts of patient degradation (Jovanov et al., 2005). In the context of the user-friendly GUI, some applications, such as iRevive, employ the metadata-driven approach that will allow users to set up the GUI layout in running time and the rule-based approach to show procedures of data collection in particular medical cases and the relationships among sampling data (Gaynor et al., 2007). These topics will be explored in later sections.

4.2.3 Tier three: medical server (database)

Tier three is responsible for aggregating and managing PCRs and assigning network channels to the local client devices (Milenković et al., 2006). For example, in the iRevive architecture, this tier preserves three kinds of data: the PCRs, the metadata and the predefined medical rules (Gaynor et al., 2007). The PCR including the patient's physiological data will be stored in the local database. It will also be available to various authenticated people, such as emergency department personnel, incident commanders and medical specialists, by employing secure web portal technology (Gao et al., 2005). The metadata includes the entry modules for the GUI of the personal server, and the rules are the metadata defining the procedure of the medical data sampling. Such clinical results can be used for further research in the field, and this medical history can be applied to current clinical operations as well (Jovanov et al., 2005). Moreover, in the iRevive architecture, when updating the PCR to or downloading them from organisational data repositories, the data transfers are subject to the Health Level 7 version 3 (HL7v3) data exchange standard (Gaynor et al., 2007).

4.3 Deployment scenarios

The wireless telemedicine with the WWBAN architecture can be configured in three ways in terms of the arrangement of wireless network devices in tier two (Milenković et al., 2006). Figure 5 shows one of three scenarios in which the wearable medical sensors and the PS running on the local client devices can communicate directly through the short-range wireless network connectivity, such as the IEEE 802.15.1 or 802.15.3/4, and the PS is connected to the home server by utilising the WLAN connectivity, such as the IEEE 802.11 standard. The home server can usually establish communication with the internet and send physiological data to the base station including some repositories at hospitals. Since the data transmission would occur on a regular basis, this type of wireless telemedicine architecture is suited for homes, the work place or the hospital healthcare.

Figure 5 WWBAN wireless telemedicine Scenario 1 (see online version for colours)

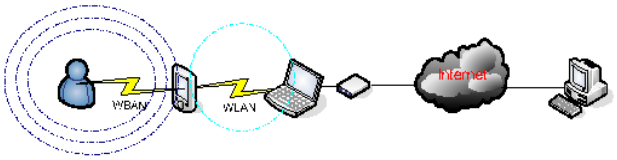


Figure 6 adds slight modifications to the first scenario. In this type of architecture, the sensor network coordinator is directly integrated into the home server that runs the PS (Milenković et al., 2006). The patient's physiological data captured by wearable medical sensors are directly transferred to the home server through the short-range wireless network connectivity. Then these data are sent to the base station at hospitals through the internet. This configuration is thus suited for home healthcare. However, although effectively cutting the cost of the client devices, this model can suffer from a higher energy consumption caused by requiring more RF output power and frequent retransmissions because of the low QoS.

Figure 6 WWBAN wireless telemedicine Scenario 2 (see online version for colours)

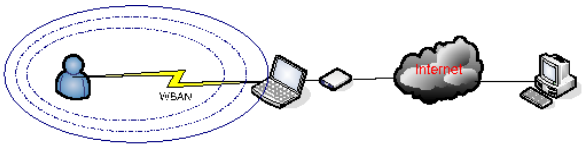
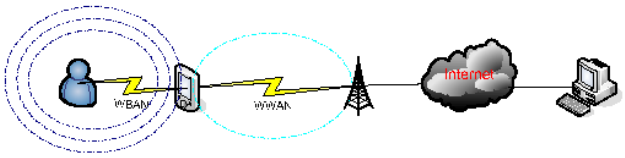


Figure 7 shows another possible modification of the wireless telemedicine architecture, in which the portable devices running the PS, such as PDAs or 3G cell phones, which can equip a WWAN interface, can establish communication with the medical server directly (Milenković et al., 2006). This configuration can allow the patient's condition to be continuously monitored locally, while patients can continue their lives as usual. Thus, doctors will be alerted immediately only when patients fall into critical conditions. This model is therefore suited for in-home rehabilitation.

4.4 Wearable medical sensor networks architectural design

In designing wearable medical sensor applications, such as a biosensor shirt (Liszka, 2007), it is required to take three levels of design framework into consideration, namely the Communication Policy (level 0), Sensing Modalities (level 1) and Diagnostic Profile (level 2).

Figure 7 WWBAN wireless telemedicine Scenario 3 (see online version for colours)



The base level is called the Communication Policy level (for bandwidth, data rate, coverage, power, etc.), and it is mainly concerned with the hardware and related software configuration (Liszka, 2007). For example, this level will establish the optimal bandwidth and computing power of medical sensors to achieve low battery consumption. That is, since not all physiological signals require high bandwidth or computing power, acquiring appropriate values of these attributes will help to reduce the battery consumption. In addition, maintenance of the sensor network connectivity or topology regardless of human movements is considered at this level. At the same time, some hardware characteristics should remain flexible. For instance, alerting users of low battery or medical emergencies should preferably be employed at the hardware level (Liszka, 2007).

The second level, the Sensing Modalities level (for 3D geometry, measurements, scheduling, algorithms, etc.) is concerned with the system architecture from the engineering perspective. At this level, one problematic issue will be to consider proper places to put biomedical sensors regardless of human movements, such as reaching, turning or bending down (Liszka, 2007). This placement strategy will largely influence the quality of the physiological data collection. On the other hand, the timing of the data collection or data transmission is another issue. Because sensors will not be required to achieve 100% of monitoring physiological data, adequate scheduling will save battery life. For example, some sensors will monitor the patient's physiological data on a regular basis, while others will capture the data only when required. Data sizes are also considered according to what kind of medical data sampling is applied. For example, two integers will be enough for sampling blood pressure, but millivolts and microvolts will be additionally required for ECG (Liszka, 2007). Likewise, an amount of local storage and a protocol used for communicating with other sensors are considered at this level.

The top level is the Diagnostic Profile level (for ECG patterns, patient history, etc.). This level is mainly concerned with observation of physiological signals (Liszka, 2007). For instance, determining what physiological parameters are required for cardiac diagnoses will be involved at this level. What heart conditions should be diagnosed and establishing their priority will also be considered. These conditions may include anomalies of heart rhythms or a cardiac arrest in progress, as well as more subtle heart conditions, such as evidence of a previous heart attack, abnormal blood electrolytes, myocarditis and pericarditis (Malmivuo and Plonsey, 1995; Rosenbaum et al., 1996; Durbin, 2000; Liszka, 2007). According to these concerns, what type of and how many sensors are required will be determined eventually (Liszka, 2007).

5 Medical peripherals for telemedicine

A typical telemedicine kit consists of a variety of medical peripherals, such as an electronic stethoscope, pulse oximeter, ECG, a video conferencing system and a Charge-Coupled Device (CCD) camera. These medical peripherals are controlled by the personal server running the local base station, e.g. PCs or PDAs. For example, (Adler, 2000), a portable telemedicine kit which was made up of a durable plastic case involved a laptop PC running custom telemedicine software that controls several medical peripherals, such as an electronic stethoscope, an electrocardiogram recorder, a medical imaging system, blood pressure, temperature and other measurements. An access panel had various plug-ins to interface medical peripherals with a laptop PC, and connections between the PC and the access panel were made under the PC.

Tablet PCs are an alternative choice for the portable telemedicine kits, and they are nothing but ordinary laptop PCs with handwriting recognition (Hackney, 2005). They can understand various handwritings by tracing the movement of a stylus directly on the display. This capability should allow medical practitioners to write their medical decisions in the traditional way (like write on paper forms) instead of typing the keyboard.

In the context of the medical peripherals (Adler, 2000), according to the previous studies by the Ministry of Health in Costa Rica in 1996 and Centre for Future Health at the University of Rochester in 1999 [Rapid Assessment Procedure (RAP)], telemedicine kits should be designed to suffice for at least the next five capabilities (Adler, 2000):

- A digital stethoscope can capture excellent condition of audio data from heart and lungs.
- A 12-lead electrocardiogram can be recorded.
- Audio-visual recorders can record video and images of the eyes, ears, nose, throat and skin with high quality.
- Blood pressure, pulse, body temperature and weight can be correctly captured.
- The PCR can be posted to and downloaded from the internet and can be electronically accessed by authenticated doctors. Instead of expensive video conferencing systems, experimental webcams are used for the two-way video data transfer (Hackney, 2005).

5.1 Electronic stethoscope

Stethoscopes are instruments with which physicians listen to a patient's heart beat and lungs to find an anomaly of the objects. With electronic stethoscopes, the sound of the heart beat and lungs, particularly the targeted frequency, are electronically amplified (Adler, 2000). According to Adler (2000), electronic stethoscopes are generally designed to capture a low frequency, which is suitable for the sound of the heart and lungs, by eliminating high frequency external noise. Moreover, electronic stethoscopes also perform sound loss and resonance effect cuts, multiple level amplification, noise reduction and frequency range extraction. This involves an audio pickup at the diaphragm and a headset.

5.2 Wearable pulse oximeter

Pulse oximeters measure the blood oxygen saturation (SpO_2), heart rate (HR) and plethysmogram waveform in non-invasive way. A patient simply inserts his/her index finger or earlobe into a plastic housing (a plastic box) (Shnayder et al., 2005). Inside the housing, they project infrared and near-infrared light on the index finger and observe how much these two kinds of lights will be absorbed by haemoglobin in the blood vessel (Shnayder et al., 2005). The extent of light absorption is then translated into the SpO_2 level (Shnayder et al., 2005). The light absorption patterns from the blood vessel expansion and contraction also represent the HR (Shnayder et al., 2005). Patients suddenly having these parameters change must receive immediate care.

The Harvard University research group created mote-based wireless pulse oximeters from commercial pulse oximetry sensor modules (Welsh et al., 2003; Shnayder et al., 2005). In one of these models, a mote, such as Mica2 or MicaZ (manufactured by Crossbow Technology, Inc.), and a pulse oximetry interface board, such as a BCI® Micro Power Oximeter Board (manufactured by Smiths Medical PM, Inc.), can connect to a standard finger housing with a serial port (Shnayder et al., 2005). Physiological signals captured by the finger housing are securely transferred to the mote through the pulse oximetry interface board. These signals are then time-stamped and encrypted with a unique node identifier and sent to a particular receiving mote (Welsh et al., 2003). Since a receiving mote can be integrated in a handheld device, medical practitioners can immediately check a patient's condition. Also, the central PC of an ambulance can receive a patient's SpO_2 or HR directly from wearable pulse oximeters. In this case, the central PC will send these data via the WLAN connectivity to requesting handheld devices which do not have a receiving mote alongside (Welsh et al., 2003).

Another type of wearable pulse oximeter is a ring-shaped device that a patient wearing it on a finger is not inconvenienced after long monitoring periods (Bonato, 2003). Since this pulse oximeter integrates a low-power transceiver, it can make a two-way communication to the base station in order to upload vital signs at regular intervals.

5.3 Electrocardiograph (ECG)

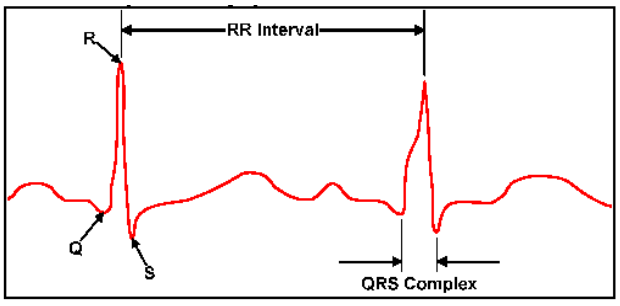
Currently, most telemedicine systems involve electrocardiographs (ECG), which are used to detect undesirable heart rhythms, blood and oxygen supplies, and excessive tension of the heart muscle (Adler, 2000). Since the heart muscle's movement is initiated by electricity, this electrical activity can be captured by surface sensors (electrodes) connected to an ECG recorder (Liszka et al., 2004b). A common ECG recorder comes with 12–15 leads with electrodes (Shnayder et al., 2005). Electrodes put on the top of leads are fixed on a patient's chest, arms and right leg and collect both the cardio rhythms and the heart's electrical impulses over short period of time.

A large bounce in an ECG waveform is reflected by the current orthogonal to the surface of an electrode. A smaller bounce in a waveform results from the current diagonally coming into the electrode surface. A biphasic bounce in a wave form comes from the current parallel to the surface of an electrode (Liszka et al., 2004a). Software running on an ECG recorder then amplifies these transferred electrical signals and visualises them on the display of the system or on a rolled paper. If a patient has undesirable heart rhythms, the software shortly notifies a physician of the patient's condition (Adler, 2000).

Attaching many electrodes over a long-time period will make a patient immobile and uncomfortable, so this type of cardiac data collection will go on for no more than 30 minutes. Occasionally, a brief data sampling will not be enough for a physician to detect irregular cardiac activity if the cardiac problems only happen once or twice a day, and these situations are frequent (Shnayder et al., 2005). In addition, since muscle contractions can also produce electricity, 12–15 lead ECG recorders are so sensitive that the results can often confuse a physician (Liszka et al., 2004a). In order to avoid these situations, a continuous ECG telemetry is additionally used in intensive cardiac monitoring (Shnayder et al., 2005). Unlike short-time ECG data collection, continuous ECG telemetry employs two or three non-obtrusive electrodes over a long period of time, and these cohesive electrodes are generally fixed on the right infraclavicular, the left infraclavicular, and possibly the left chest below the mammilla to record three angles of the heart's electrical activity (Liszka et al., 2004a).

The primary heart rate and QRS interval can be sufficiently provided from these two or three electrodes. A QRS interval is the interval between the contractions of the ventricles, i.e. the strong part of the heart beat (Durbin, 2000). From these data and the R-peak detection algorithm, the continuous ECG telemetry is enough to detect arrhythmia disorders, such as bradycardia, tachycardia, sinus arrest, ventricular tachycardia with broad QRS complexes and superventricular (Pan and Tompkins, 1985; Liszka et al., 2004a). Figure 8 shows the RR-interval and the QRS complex from a theoretical ECG signal. Preferably, it automatically notifies physicians if these anomalies occur.

Figure 8 Theoretical ECG signal (see online version for colours)



5.4 Wearable ECG sensor

The wireless configuration of the ECG recorder enhances the portability of the ECG sensor and enables ambulatory cardiac healthcare in homes or work environments. Although the first-generation wireless of ECG telemedicine could use only short-range wireless connectivity and was limited to hospital use, the next-generation wireless of ECG

sensors could allow cardiac monitoring to be out of hospitals or in homes by periodically sending the data directly to physicians via the internet (Liszka et al., 2004a). At this point, however, it was still difficult for physicians to achieve real-time cardiac data access because of its expensive cost and time requirements. To establish the real-time data collecting configuration, NASA and Case Western Reserve University's Heart & Vascular Center developed the Arrhythmia Monitoring System (AMS) (Liszka et al., 2004a). The AMS enables a real-time ECG data collection from mobile patients by exploiting digital, packet-switching telephony services in metropolitan areas (Liszka et al., 2004a). This system can also detect the current position of a patient from GPS location data (Liszka et al., 2004a).

5.5 Motion analysis system and EMG

A primary objective of the motion analysis systems is to record muscular activity and limb movement. Particularly, the physical rehabilitation resulting from brain damage and Parkinson's disease treatments are aided by this system (Shnayder et al., 2005). Brain damages, such as internal bleeding or a critical shortage of blood, eventually result in temporary or functional termination of the partial brain. This causes patients to have partial movement disabilities. Parkinson's disease is also a physical impediment that causes a tremor or unintended shaking of the body. Parkinson's disease potentially starts with brain injuries or infections. The unintended movement from these diseases should be accurately watched on a regular basis so that doctors can prescribe medicines for the diseases in a proper and timely fashion.

The motion analysis systems have a variety of sensors which are placed on particular body segments. There are mainly three types of sensors, an accelerometer, gyroscope and surface electrode for EMG, and these sensors are used to capture the relationship between body segments, the angular velocity and the electrical field that appears during the movements, respectively (Bussmann et al., 1998; Bonato et al., 2003; Mathie et al., 2004; Shnayder et al., 2005).

5.6 Wearable motion analysis system

As in other physiological sensors, wearability is ideal for the prolonged motion analysis. In the use of a mote-based motion analysis system, each node will be placed on the upper arm, lower arm and torso (Shnayder et al., 2005). A very small module incorporated with the accelerometer, gyroscope and EMG unit will amplify electrical signals and will simultaneously reduce some noises. After that, it will relay signals to a mote attached alongside, and the mote will transmit the data to a user device. Since multiple modules are working together on a patient's body simultaneously, data must be properly time-stamped for synchronisation.

5.7 Medical imaging system

Medical imaging is essential to the telemedicine system. A possible way to use medical imaging systems is to let doctors and patients have remote audio-visual communication. In this case, the medical imaging systems must have the capability of not only video transfer, but also of audio data transfer, in order to allow conversations between doctors and patients. When telemedicine systems equip a standard PC, a webcam is a possible medical imaging system. For example (Hackney, 2005), the University of Virginia research group examined the usage of a webcam for wireless telemedicine. This telemedicine kit utilises an USB-connected webcam to allow face-to-face communications in a video conference. A webcam also has a small microphone at the top.

Because this type of imaging system is mainly used for the medical interviews and may not have the high resolution of video images, some telemedicine systems can complement it by additionally utilising a CCD camera for intensive viewing. For example the medical imaging system in the LINCOS project consists of a 410,000 pixel medical one-fourth CCD camera along with a lighting source which costs about $4000 and followed FDA regulations (Adler, 2000). This FDA approved CCD camera (distributed by American Medical Development in Lowell, MA) featured Automatic Gain Control (AGC), polarisation, 1–200x zoom range, white balance and freeze-frame.

The video conferencing standard H.323 is mostly used in the telemedicine field because it accommodates the internet protocol (IP), which can be recognised by most of the computing devices (Hackney, 2005). According to the defined H.323 audio-video minimum bit rate (5.3 Kbps for the audio and 64 Kbps for the video), it shows that, in theory, at least nearly 100 Kbps of the data transfer is required. Since some local wireless broadband services can provide a maximum 1.5 Mbps for the downstream and 550 Kbps for the upstream, this wireless connectivity will be capable of manipulating the minimum audio-visual bandwidth of the H.323 video conferencing standard. In fact, in previous preliminary experiments, the University of Virginia research group successfully accomplished the real transmission of one-way video streaming by using a local wireless broadband service. Table 1 shows throughputs (kbps) of the two-way video streaming provided by the later experiments at The University of Virginia (Hackney, 2005).

Table 1 H.323 average throughput

Video (OUT)	*Video (IN)*	*Throughput (OUT)*	*Throughput (IN)*
Sub-QCIF	Sub-QCIF	226.31 kbps	143.36 kbps
Sub-QCIF	QCIF	261.12 kbps	346.11 kbps
Sub-QCIF	CIF	221.18 kbps	599.04 kbps
QCIF	Sub-QCIF	287.74 kbps	148.48 kbps
QCIF	QCIF	284.67 kbps	323.58 kbps
QCIF	CIF	319.48 kbps	576.51 kbps
CIF	Sub-QCIF	508.93 kbps	185.34 kbps
CIF	QCIF	523.26 kbps	297.98 kbps
CIF	CIF	543.74 kbps	501.76 kbps

Source: Hackney (2005)

5.8 Georgia Tech Wearable Motherboard

The Georgia Tech Wearable Motherboard is a cloth which captures a patient's heart rate, temperature, motion, position and barrier penetration (Bonato, 2003).

5.9 Consumer-centred telerehabilitation

Consumer-centred telerehabilitation consists of video conferencing, wireless communication tools and expert systems to offer support for a patient's rehabilitation. The system gathers a patient's physical data concerning their movement, which is monitored by video conferencing. The expert systems then organise the movement by neural networks and fuzzy logic. IEEE 802.11b (wLAN), Bluetooth (wPAN) and cell phone technology (wMAN) are utilised as the wireless connectivity (Bonato, 2003).

5.10 Ambulatory electroencephalography

Wearable systems are also applicable to Ambulatory Electroencephalography (AEEG), which concerns epilepsy. Since a patient is always threatened by a sudden seizure occurrence, this AEEG, like other wearable devices, can make an extended observation of a patient in order to make an effective diagnosis and support seizure control. Moreover, the recent fast processing algorithms enable AEEG to detect the unique habits of patients' seizure events (Bonato, 2003).

6 Wireless telemedicine applications

In this section, we review some wireless telemedicine applications. Before going into the details of each appliance, we give an overview of their main features in Table 2.

6.1 Nurses' work and wireless wearable devices

In order to have effective telemedicine, it is essential to understand the needs of doctors and nurses. Drugge et al. (2006) described a way to understand nurses' work as follows. A group of nurses were accompanied for a day and observed while working to know what nurses face in day-to-day situations: (a) taking blood samples from patients and giving medications to the patients; (b) writing reports in their charts and storing them in computers; (c) talking to a patient's previous attendants via mobile phones in cases of urgency in order to reduce the time gap of knowing the patient's previous condition and treating the patient. Failure to communicate hurts both nurses and the patient. The problems are summarised by the following observations (Drugge et al., 2006): (a) communication; (b) information dissemination; (c) access to patient charts; (d) organisational issues. Communication and information dissemination are closely related and are the major problems (Drugge et al., 2006). One major goal is to develop a mobile tool to collect/store/disseminate all patient information.

Table 2 Wireless telemedicine applications

Name	*Features*	*Scope*	*Tech.*	*Environment*
AMON	Low-cost, low-power, wearable device	Monitor the patients' health and store the information	MASN, three-lead ECG	Nurses' work, Hospital
BASN (BAN)	Wearable PDA, implanted sensor	Optimise information and resources	Body area network	Home, Hospital
IPI Encryption	Biometric features	Identify sender, secure network for telemedicine	Cryptography	Hospital
AGAPE	Interact with people near-by	Track elders in outdoor activities	MANET	Medical emergency
RFID	Unique ID, convenience	Identify the user, locate the mobile patients	RFID	Home, Hospital
CodeBlue	ADMR, a simple query interface, location tracking	Establish flexible, scalable and robust medical care network	Three-lead ECG, motion analysis, ad-hoc	Medical emergency
iRevive	Handheld device	Aggregate medical data	Ad hoc	Medical emergency
Euro Healthcare	Mobile units and consultation units	Provide better healthcare in emergency case	Satellite, GSM, POTS or ISDN	Medical emergency
Wireless Tele-radiology	Equips two mobile vans	Provide better healthcare in emergency case	Satellite, ATM, ISDN, CT	Medical emergency
NASA Project	Under Microgravity	Record electro-physiological heart changes in microgravity area	PUMA, EWT, MRDL, CCSDS	Microgravity Environment
AMS	Central server, long-distance communication	monitor heart muscle's electrical activity	Thee-lead ECG, Bluetooth, GPS	Medical emergency
Biosensor Shirts	Unobtrusiveness, non-contact ECG electrodes	Enables patients to be free from a sense of devices	Miniature motes	Home, Hospital

Wearable computers are used to monitor the patients' health and to store information such as AMON (Drugge et al., 2006) from the Wearable Computing Lab at ETH Zurich (www.wearable.ethz.ch), Switzerland. Monitoring patients simplifies both patients' daily lives and medical personnel's work. Recently, Hu et al. (2008a, 2008b, 2008c) have taken advantage of modern low-cost, low-power sensors and wireless communication technology to create a telecardiology sensor network for remote ECG monitoring purposes. This network is a Medical Ad hoc Sensor Network (MASN) system. They use a practical MASN hardware/software platform to perform real-time healthcare data collections. Based on Wireless Sensor Network (WSN) technology, the wearable mobile platforms are distributed to patients of concern. These mobile platforms are responsible for gathering patient vital signs by using a three-lead ECG monitoring system. Then, the gathered data are transmitted wirelessly via radio to the receiving station, which is connected to a workstation where the data are processed. ECG feature extraction/classification techniques are applied to the patient data and the characteristic points of interests are extracted. These data provide meaningful information for the diagnosis of possible cardiovascular diseases (Hu et al., 2008a; Hu et al., 2008b; Hu et al., 2008c).

Pervasive computing can be used by nurses. It will be interesting to know what kinds of systems, involvement and encouragement of end users in designing the interaction with prototypes. Consultation, diagnosis of illness, monitoring of treatment processes and even conduct of surgical operations should be further improved (Istepanian et al., 2004).

6.2 Online prototype and BAN

Another idea is to develop an online prototype with live software and hardware (Gemperle et al., 1998). A wearable PDA is strapped around one's waist and hip area (Gemperle et al., 1998). Wireless technology, such as a Body Area Sensor Network (BASN) or Body Area Network (BAN) (Poon et al., 2006), can be used to optimise the resources and to enhance the control and programming of the overall system to adapt to the body condition and the external environment. Sensors, or devices, are connected to share information and resources in BAN, and sensors are worn on or implanted in a person's body. A common network connecting all of the nodes is needed when a body is connected to many sensors to collect all of the information and pass it to a remote person. The doctors in Shanghai Eastern Hospital use such a device to facilitate their daily work. That device is a small PDA with 54 Mbps wireless bandwidth that stores the patients' information (Wang and Gu, 2009).

6.3 Security and interference

Data manipulation, eavesdropping and injection may happen in an unsecured telemedicine network. It is dangerous to the life of a patient to be wrongly treated. Assuming a robust key, Cherukuri et al. (2003) proposed a secured key distribution mechanism using a biometrics approach, in which a biometric trait, obtained from the system, is adopted as a key for data transmission. Biometric is a technique commonly defined as automatic identification or verification of an individual by his/her physiological or behavioural characteristics (Jain et al., 2004). For example an Inter-Pulse Interval (IPI) can be used as a trait for securing the BASN network. Based on the secure key transmission scheme (Cherukuri et al., 2003), Liszka et al. (2004a) used physiological signals to generate an encryption key for BASN. The IPI's randomness was validated via the calculation of the entropy, arithmetic mean value, chi-square, etc. (Bao et al., 2005). It can be useful to authenticate the same network by identifying the nodes, and the nodes can also identify each other by using the same biometric code (Bao and Zhang, 2005). A biometric trait can further be applied to humans for different characteristics of different people, and BASN can be better secured by using human biometric traits as authentication keys.

ECG and photoplethysmogram (PPG) were collected in experiments to estimate blood pressure via channels sampled at 1000 Hz, and the IPI was obtained from the ECG by estimating the time interval between two R waves (Poon and Zhang, 2005). A set of biometric traits is defined $B_t = \{b_{1t}, b_{2t}, \ldots, b_{nt}\}$, where t is time and b_{it} $(1 \le i \le n)$ is a binary sequence obtained at time t to represent a biometric trait at node i.

Albeit IPI has been shown to be successfully used for securing a BASN, it must satisfy the following seven criteria for any human physiological or behavioural characteristic to be used in a practical biometric system (Poon et al., 2006): (a) universal: the majority of the entire population should possess the characteristic; (b) distinctive: the characteristic should be sufficiently different on any two individuals, i.e. it must be similar but not the same; (c) permanent: the characteristic should be sufficiently invariant, with respect to the matching criterion, over a reasonable period of time; (d) collectable: the characteristic should be easily collected and measured quantitatively; (e) effective: the characteristic should yield a biometric system with good performance, i.e. given limited resources in terms of power consumption, computation complexity and memory storage, the characteristic should be able to be processed quickly with recognised accuracy; (f) acceptable: the characteristic should be widely accepted by the general public as an identifier in their daily lives; (g) invulnerable: the characteristic should be relatively difficult to be reproduced so that the biometric system cannot be easily circumvented by fraudulent acts (Poon et al., 2006). It is easy to obtain a biometric trait satisfying all of the above conditions except for the last two. Since they are obtained easily from the human body, they are comparatively inexpensive and can also be processed easily because they are simple in nature and the resolution is also low (Poon et al., 2006). This means that accessibility is not an issue and that calculating IPI for securing data transmission will hardly increase the required terminals (Poon et al., 2006). The last characteristic is probably the most difficult, as it requires working in the most difficult environments. Furthermore, the randomness of the biometric key makes BASN different from ordinary networks. It can be obtained simultaneously and independently and need not be stored permanently. Therefore, it can be used for authenticating an encrypted key. If the key changes over time a new key can be set in its place and secured (Poon et al., 2006). The use of

biometrics in BASN can be extended to using other physiological parameters as traits in securing these networks as long as they satisfy the above conditions. IPI can be measured from sensors implanted in the body parts or externally without much variation. There are many other related security aspects (Abbes et al., 2010; Chen et al., 2010; Guo et al., 2010; Schrader et al., 2010; Zhuang et al., 2010; Kundur et al., 2011; Kalogridis et al., 2011; Li et al., 2011; Ramsey et al., 2011; Xiao, 2011; Zhang and Gunter, 2011).

6.4 Assisting elderly people

The growth rate shows an increasing population of elderly people (United Nations Population Division, 2001), and it therefore becomes a duty to care for them. The emergence of wearable devices and Mobile Ad Hoc Networks (MANETs) has provided ideal ways to improve elderly healthcare. Wearable devices help a great deal in guiding the elderly people through their daily routine, to take their medical care and to constantly monitor the person's health in detail (Abowd et al., 2002; Helal et al., 2003; Dishman, 2004).

Care for the elderly should be provided both at home and in mobile environments. Setting up equipment for an outdoor environment is not easy because it requires many tools and extensive outdoor equipment to care for these elders and to determine their exact locations so that they can receive immediate care in the case of an emergency. These tools must also be able to interact with near-by people that come to the aid of the elders in the case of an emergency and the closest hospital staff. A group level management solution (AGAPE) is proposed for outdoor assistance of the elderly in emergency situations (Rowstron and Druschel, 2001).

Systems for tracking elderly people with wearable devices may be complicated due to the mobility of elderly persons. For example (a) passengers may be in a situation to provide them with emergency care; (b) they form an ad hoc group that moves from one place to another; (c) different elderly people may have devices with different power, bandwidth, capacity, memory, etc. One principle of AGAPE (Rowstron and Druschel, 2001) is context awareness, which is useful for above issues (a) and (b). Healthcare for elderly people is essential. AGAPE is a good solution to such a challenge, as it effectively addresses most of the challenges in designing such a network. The AGAPE network is being tested and showing promise in the development of care for the elderly (Rowstron and Druschel, 2001).

6.5 Hospital integrated and home care network

A hospital-integrated network can provide both typical information technology applications (such as web browsing, email, etc.) and medical applications including: medical IT (such as image and video transfer, patient record access); medical telemetry for patient monitoring; remote control of medical devices (such as infusion pumps controlling drug delivery and ventilators controlling physiological functions); and real-time multi-media applications (such as voice and video conferencing used for remote medical procedures). Wireless technologies can be used to deliver information to bedside monitors. High-bandwidth wireless networks can send high throughput secure data. Sharing a single integrated infrastructure among different applications is complex because some applications are critical to the life of the patient.

A home care environment is important for recovery of patients. Wireless services become ubiquitous and the cost of providing health services grows. Some non-critical medical services can be offered away from hospitals, i.e. elderly care in homes using wearable wireless telemetry devices connected to WiFi that generate local alarms or send information to a remote monitoring/emergency centre via the internet. Applications such as remote real-time consultations can also be supported.

6.6 RFID in telemedicine

Xiao et al. (2006b) described two applications using RFID: the first application is to study supply and demand in hospitals and healthcare; the second application is mobile telemedicine using smart sensors. In the first application, supply and demand can be studied regarding doctors, nurses and patients in hospitals and healthcare services (Xiao et al., 2006b). Doctors, nurses and patients have RFID tags attached so that bottlenecks of supply and demand among them can be identified and improvements can be made possible. RFID tags can be plastic bands strapped onto wrists. In the tags, only an ID is stored to reduce security and privacy attacks. The unique ID is associated with a database record saved in a server connected to RFID readers. In the database, the record of a patient may include the patient's name, date of birth, gender, a medical record number, billing, medical insurance, pharmacy and so on (Xiao et al., 2006b). RFID readers can be fixed in each room or mobile in tablet-style PCs with wireless LAN connections. For doctors and nurses, tags are embedded in their access IDs, which are normally used to access various rooms (Xiao et al., 2006b).

In the second application Xiao et al. (2006b) proposed a real-time patient monitoring system that can use smart sensors to collect patients' vital signs so that medical specialists can perform remote diagnoses anywhere and at any time. Intelligent location tracking functions will also be incorporated to locate mobile patients in the case of an emergency (Xiao et al., 2006b). This system can substantially reduce response time to medical emergencies and improve the accuracy of remote diagnosis. The impact of the real-time patient monitoring system can be tremendous in benefiting healthcare providers, the entire healthcare industry and in improving the health of our society (Xiao et al., 2006b). The system can also be used in a variety of other important applications, from monitoring soldiers' conditions on a battlefield to tracking relief workers in a disaster area (Xiao et al., 2006b). A large number of microsensors can be attached non-invasively to patients to collect ECG, pulse rate, basal temperature and other vital signs. RFID tags are used to identify patients' locations so that, in the case of an emergency, patients can be found easily (Xiao et al., 2006b). These medical sensors can transmit their data wirelessly to some special sensors, called cluster heads, for further processing. The processed data are then transmitted to a

tablet-style PC, a wireless PDA or a cellular phone. These devices not only display and store the data locally, but also forward the data to remote medical specialists over a WLAN/Metropolitan Area Network (MAN) or cellular network. Medical specialists can monitor patients' vital signs anywhere and at any time, and can perform remote diagnoses, as well as commands/queries to the sensor network (e.g. to activate more sensors in a particular area). Intelligent location tracking functions using RFID are adopted to locate mobile patients in the case of an emergency. In a typical ambulance system, a camera takes an ambulance patient's video clips and transmits them to the consultation unit of a medical centre (Xiao et al., 2006b). At the same time, the Emergency Medical Paramedics (EMPs) use a wireless cellular connection to talk to doctors or medical professionals. An ambulance workstation continuously collects data from the patient's body and sends it to the doctors (Xiao et al., 2006b).

6.7 Ad hoc medical sensor networks: CodeBlue, iRevive and AID-N

One application of the telemedicine system with the WWBAN is use in mass casualty disasters. In the sudden occurrence of large earthquakes or tsunamis, the number of victims will increase rapidly, and the number of victims on site will quickly overwhelm the emergency medical staff. Besides, the victims and emergency medical personnel will move around the field restlessly during the aftermath of a mass casualty disaster (Malan et al., 2004). In that case, establishing sensor medical networks relying on the fairly stable low-band wireless connectivity among a few immobile devices is a bad choice (Malan et al., 2004). In addition, it may be hard to find a local WLAN or wireless WAN.

In disaster scenarios, instead of looking after every patient in order, wireless telemedicine kits will be distributed to every victim. This wireless telemedicine kit contains a set of basic physiological sensors and utilises the WWBAN connectivity between the sensors and the personal servers. The physiological sensors worn by the victims will automatically start recording physiological signals and transmit their current conditions to emergency medical personnel in real time. Moreover, since these physiological sensors notify the existence of victims in critical condition and their locations, practitioners can prioritise victims in critical condition (Shnayder et al., 2005; Welsh et al., 2004; Welsh, 2005). However, since communication between vital sensors and the personal server is basically established by a low-power, single-chip radio, such as the IEEE 802.15.1 or IEEE 802.15.4, the connectivity would be restricted to a short-distance and can have trouble with the long-distance wireless communication. Thus, unique network protocols and configurations are required to enable multi-hop sensor communications or to discover destination devices.

To achieve medical care in a mass casualty disaster, the Harvard University research group designed CodeBlue, a wireless communication infrastructure (Malan et al., 2004; Shnayder et al., 2005). CodeBlue aims to establish flexible, scalable and robust network connectivity in the ad hoc style (Malan et al., 2004). CodeBlue has some unique features, such as ADMR, a simple query interface, a device discovery protocol and a location tracking system (Shnayder et al., 2005; Malan et al., 2004). In its current state, CodeBlue prepares for two kinds of physiological sensors, such as pulse oximeters and three-lead ECGs, and motion analysis boards. The scalability of CodeBlue allows it to be adaptable to both the regular operations in a clinic (a scarce situation) and to a mass casualty location (a dense situation) (Malan et al., 2004). Regardless of these advantages, CodeBlue still has many issues: the limited memory, computational power and radio bandwidth of each node (Chen et al., 2006). Hu et al. (2008a) designed a wearable ECG monitoring platform based on a three-lead system and a design under the CodeBlue project. The ECG data are collected using the mobile platforms that are transmitted wirelessly using Tmote Sky via radio frequencies to a receiving mote connected to the workstation monitor. The received patient data are then processed using wavelet transformation to provide feature extraction capabilities in order to locate the characteristic points of the ECG waves (Hu et al., 2008a). Thus, we are able to expect the patient's physiological status, which can help reduce response time in emergency situations.

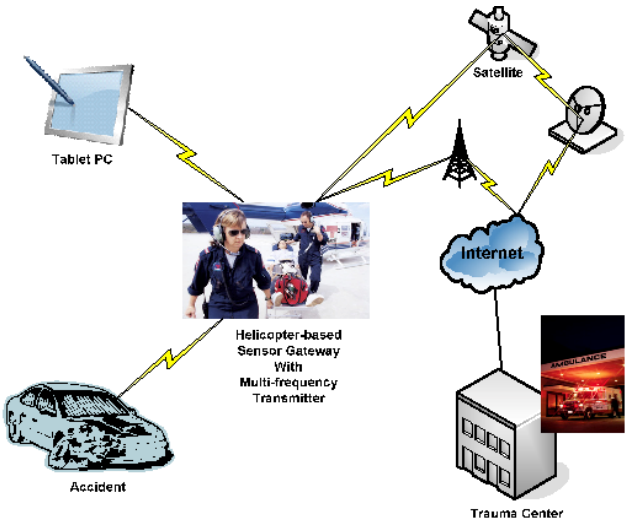
Similarly, iRevive is the ad hoc medical sensor network application that is now being researched by collaboration of 10BLADE, the University of Arizona, and Boston MedFlight (Gaynor et al., 2007). iRevive mainly concerns prehospital situations and aims to dynamically build the telemedicine system architecture by running the PS on a variety of handheld devices, such as tablet PCs or PDAs. iRevive addresses three objectives: the aggregation of medical data from a variety of medical sensors and human manual input, flexible user interface and rule-based user inputs. Particularly, several wearable medical sensors, such as wireless pulse oximeters or ECG sensors, will continuously transmit the patient's physiological data to the practitioner's handheld devices through the short-range wireless network connectivity. The practitioners will control these medical sensors and process the data through the PS (Gaynor et al., 2006; Gaynor et al., 2007).

These real-time PCR and human manual inputs will be gathered in the sensor gateway and then updated to the organisational database through a web application that is subject to the Health Level 7 version 3 (HL7 v3) data exchange standard, as shown in Figure 9 (Gaynor et al., 2007). Similarly, the PCR can be referred to by the authenticated personnel with the HL7 v3 (Gaynor et al., 2007).

John Hopkins University used the Advanced Health and Disaster Aid Network (AID-N), which was designed to support mass casualty patient monitoring, patient record generation and remote patient record review (Gao et al., 2005). The system basically consists of wireless network communication, the central server, several wearable sensors and handheld devices running a prehospital patient care software package (MICHEALS). The wearable sensors cover the real-time physiological data monitoring and transmitting, location tracking, medical record storage and

triage status tracking. Real-time vital signals offered by the wearable sensors will be observed and examined by the MICHEALS running on a handheld device. Compared to the alert detection parameters, shown Table 3, if these signals indicate something abnormal, the MICHEALS will immediately draw the practitioner's attention to the patient by either sounding a buzzer or blinking an LED.

Figure 9 iRevive use case (see online version for colours)



Source: Gaynor et al. (2007)

Table 3 Alert detection parameters

Alert Type	*Detection Parameter*
Low SpO_2	$SpO_2 < 90\%$
Bradycardia	HR < 40 bpm
Tachycardia	HR > 150 bpm
HR change	ΔHR/5min > 19%
HR stability	Max HR variability from past 4 readings > 10%
BP change	Systolic or diastolic change

Sources: Behrman (2000), Chobanian et al. (2003), Gao et al. (2005), Palatini (1999) and Schwartz (1999)

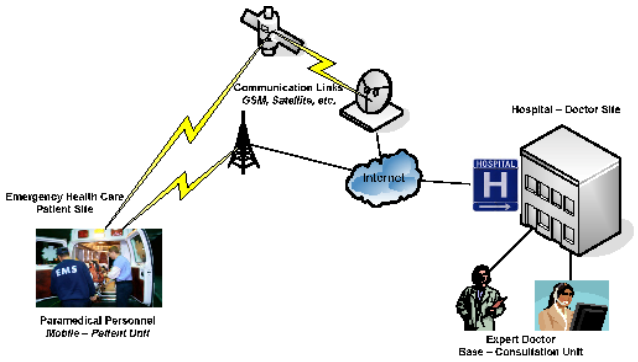
The MICHEALS is also capable of storing the PCR into the on-board memory in the motes. This capability allows other practitioners to take over the patient by loading the PCR on their PS (Gao et al., 2005). The PCR will be stored in the local database via the local wireless networks and will be available to various authenticated people, such as emergency department personnel, incident commanders and medical specialists via a secure web portal. The AID-N involves various mote-based medical sensors, such as the pulse oximeters, blood pressure sensors and electronic triage tags (Gao et al., 2005). The transmission between these medical sensors and the handheld devices relies on the IEEE 802.15.4 based protocol (Chen et al., 2006).

When responding to a mass casualty disaster, medical practitioners will distribute to every patient the AID-N packages that include the mote and several wearable medical sensors (Gao et al., 2005). The motes will be wrapped about the patients' wrists, and the wearable sensors will be placed on appropriate parts of the patients' bodies. The sensors will then start recording the patients' vital data and automatically transmit them to the PSs occupied by the practitioners.

6.8 *Wireless telemedicine for emergency healthcare*

Some European countries have employed the Ambulance and Emergency-112 project for emergency healthcare since 1998 (Pavlopoulos et al., 1998; Kyriacou et al., 1999; Antoniades et al., 2000; Kyriacou et al., 2001; Pattichis et al., 2002). These two systems are mainly composed of mobile and consultation units, as shown Figure 10 (Pattichis et al., 2002). The mobile units are patient side components that are responsible for capturing patients' physiological signals, such as ECG, BP, HR, SpO_2 and temperature, as well as images at the patient site. This unit has a variety of wireless connectivity, so it can access consultation units through satellites, GSM, POTS or ISDN. The consultation units are components which are located at the doctor's side at a hospital or clinic and are operated by medical experts. The medical experts can remotely instruct local practitioners regarding the capture of patients' physiological data or images and the treatment of symptoms. By these prehospital cares, the mortality rate of patients has been reduced in European countries.

Figure 10 Ambulance and emergency-112 Project (see online version for colours)



Source: Pattichis et al. (2002)

6.9 *Wireless teleradiology*

Wireless telemedicine is currently applied to teleradiology, e.g. whole body spiral computed-tomography (CT) scanning (Pattichis et al., 2002). This system equips two mobile vans. One of them contains a CT scan, while the other contains equipment used for satellite communication. The CT scanner screens people for lung diseases. Image data recorded by the CT scanner will then be transmitted to a consultation centre via a satellite or the ISDN with Asynchronous Transmission Mode (ATM). Because the second van equips a teleconferencing system, medical practitioners can also get in touch with various specialists at the consultation centre in real time. Along with the CT scanner and teleconference system, a PC, image printer, facsimile machine and resuscitation system are also equipped in the van.

6.10 Project rescue of NASA

NASA initiated a project to develop a heterogeneous sensor network to support biomedical research on the ISS. An objective of this biomedical research is to record electrophysiological changes of the heart due to long-term exposure to the microgravity environment. These changes are monitored either locally or remotely (Liszka et al., 2004b). As a result of long-term exposure of the body to microgravity, the astronauts' heart will get bigger and thinner, and this situation will prevent the heart from working effectively and will cause it to get less blood than it requires, which will cause cardiac arrhythmias. The ISS deploys a 14-lead ECG sensor to detect cardiac anomalies from microvolt T-Wave Alternans (TWAs) (Rosenbaum et al., 1994) and prolonged QT-intervals (Liszka et al., 2004b).

Besides monitoring electrophysiological changes of the astronauts (Project Rescue), two other experiments are also conducted on the ISS: one measures the astronauts' body metabolisms [(Portable Unit for Metabolic Analysis (PUMA)], and the other detects irregular physiological conditions by eye examinations (INI-Tech) (Liszka et al., 2004b). Unlike on the ground, the astronauts cannot exercise efficiently on the ISS under microgravity, and the duration of bones and muscles will therefore be degraded. For example from the research, 1.0–1.5% of bone mass is reduced during MIR and ISS missions (Turner, 2000). To measure the metabolic function or physical response to the exercise, the ISS crews utilise a PUMA. A PUMA measures body temperature, flow and pressure by using prototype oxygen, CO_2 and flow sensors, and these parameters are translated into a quantified metabolic function (Liszka et al., 2004b). Moreover, since astronauts are exposed to the danger of cosmic radiation in space due to the lack of a magnetic field that reduces the harmful effects of radiation on Earth, damages of the basic cell DNA structure will result. Thus, ISS employs the INI-Tech, which is a non-invasive optical sensor that looks like a night-vision goggle with miniature fibre optic probes inside and will make early discoveries of irregular conditions of the eyes and brain by analysing fluids, tissues and blood vessels (Liszka et al., 2004a; Liszka et al., 2004b).

These vital sign sensors are connected to personality module processors by a serial link. These processors are integrated into a Compact PCI backplane, as shown in Figure 11. A personality module processor can have enough storage to monitor vital signals for 6 hours, which enables almost seamless data sampling (Liszka et al., 2004b).

The access point to or from the ground facilities on Earth, as shown in Figure 12, is an experiment processor plugged into the Compact PCI backplane. Collected physiological data will be transmitted through the ISS Medium Rate Data Link (MRDL) to the Tracking and Data Relay Satellite System (TDRSS) depending on the temporal bandwidth availability, as shown in Figure 12. An experiment processor can also has long-term storage, Embedded Web Technology (EWT) and a TCP/IP or CCSDS data link to communicate with other spacecrafts (Ponyik and York, 2002). The EWT can allow all of the personality modules to be usable with URLs from the ground facilities.

Figure 11 Project rescue system architecture (Liszka et al., 2004b) (see online version for colours)

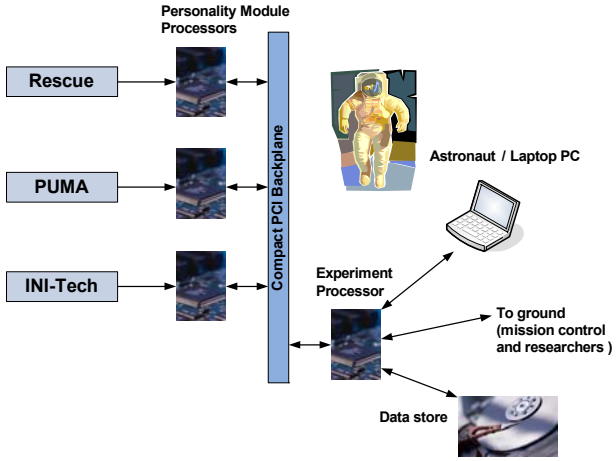
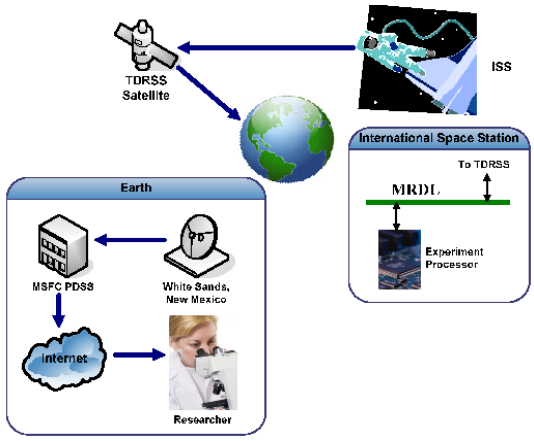


Figure 12 PRS ground communication architecture) (see online version for colours)



Source: Liszka et al. (2004b)

6.11 Arrhythmia Monitoring System (AMS)

As in standard telemedicine systems, the AMS, shown in Figure 13, has electrodes of a three-lead ECG sensor attached to certain segments of the patient's body that monitor the heart muscle's electrical activity. An ECG holder integrates the wearable server that controls ECG sensors and sends it to the central server and will be generally worn by patients, as shown in Figure 14. The wearable server and central server are mainly connected over a short-distance RF wireless communication channel, namely Bluetooth. Bluetooth uses the licence-free ISM frequency band between 2.4 and 2.4835 GHz and the frequency hopping strategy (Liszka et al., 2004a). However, because the ISM band is licence-free, devices that actually share this band range are so numerous that they inevitably suffer from signal collisions and corruption.

The central server works as the logical midpoint between patients and the call centre, as shown in Figure 15. The central server mainly performs three functions: data compression, patient position detection through GPS signals and arrhythmia detection. The central server also serves as the wireless gateway to the long-distance RF wireless communication channels, such as the General Packet Radio

Service. ECG data are continuously sent to the call centre. As a prototype of the central server, a Palm PDA is utilised in such a way that it can be connected to a private network and assigned a private internet Protocol address. By using this connectivity, the central server, shown in Figure 16, will continuously transmit physiological data to the call centre until an acknowledgement is received. However, since a fee is charged according to the quantity of the data transmitted and ECG data streaming expends the substantial bandwidth of the network, the reduction of communication time and cost is a very important issue. Although the prototype only informs patients of arrhythmia detection with an LED, it is preferable to notify with sound and automatically to make a 911 call in the case of an absence of the call centre (Liszka et al., 2004a).

Figure 13 Arrhythmia Monitoring System (AMS) system architecture (see online version for colours)

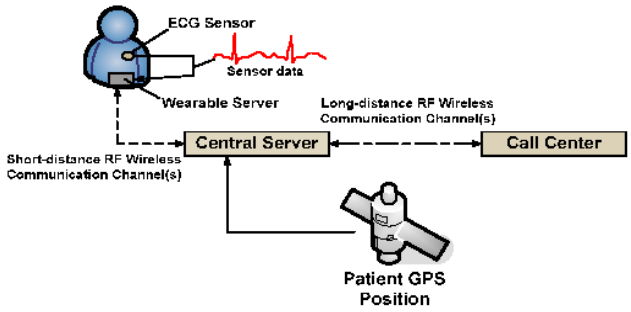


Figure 14 Wearable server for the AMS (see online version for colours)

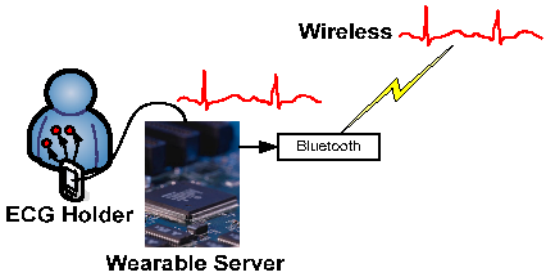


Figure 15 Call centre for the AMS (see online version for colours)

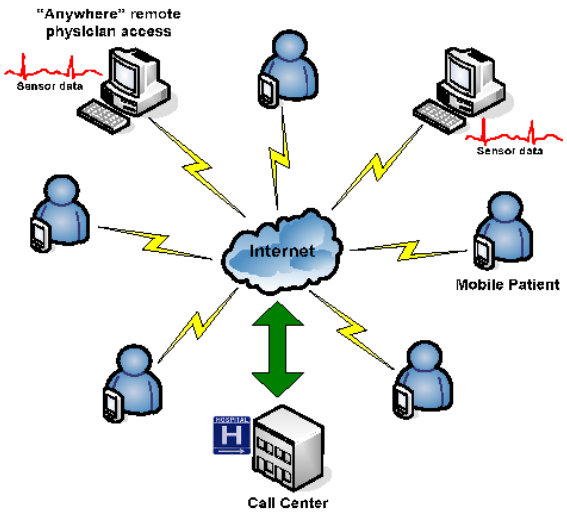
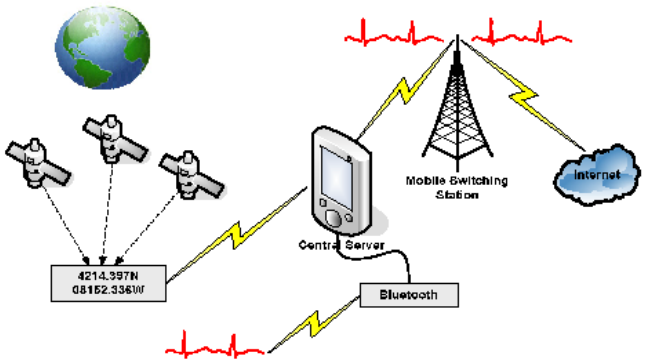
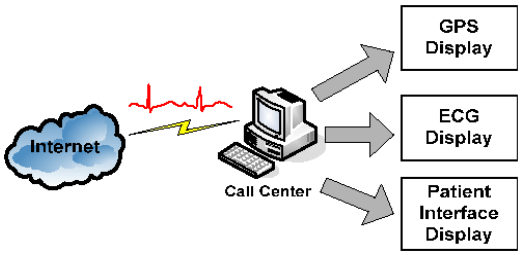


Figure 16 Central server for the AMS (see online version for colours)



At the call centre, shown in Figure 17, qualified healthcare professionals constantly monitor a set of ECG data by using traditional strip chart graphics. Patients' data are classified by their geographical area (Liszka et al., 2004a). If a patient suddenly has a heart flutter, the central server provides a button for a non-critical alert to the call centre. Moreover, when a panic button is pressed, personnel at the call centre will call a 911 service and they can help the patient through particular GPS signals by applying patient position detection.

Figure 17 Call centre for the AMS (see online version for colours)



The prototype of AMS is accompanied by a GPS transceiver with a 1.5 GHz GPS antenna and a 2.4 GHz Bluetooth antenna. A location given by GPS signals will be processed by the GPS transceiver and then sent to the PDA using the Bluetooth wireless network connectivity. The GPS location error is usually no more than 10 metres (Liszka et al., 2004a). Hence, this function will be utilised in patient position detection in emergency cases.

6.12 Biosensor shirts and wireless non-contact ECG electrodes

One goal of the wearable medical sensors is that patients feel free from a sense of equipment. In a sense, a current ECG achieves such unobtrusiveness due to the size of its miniature motes. A mote accompanied by an ECG sensor board easily resides in a human body, while an electrode can attach to body parts and collect patient heart activity continuously. For extended monitoring, however, this method still does not accomplish the perfect unobtrusiveness of medical sensors. In extended monitoring, a patient, particularly an elderly one, can suffer from skin damage due to the adhesiveness of the electrodes (Liszka, 2007). This is because, in order to achieve a

high-quality trace, a conductive adhesive gel is applied to the ECG electrodes, and these electrodes will damage sensitive skin of the elderly.

Wireless non-contact ECG electrodes are now under research. One example of such electrodes is a biosensor shirt, which is a stiff vest with a number of fixed miniature motes attached to wireless non-contact ECG electrodes (Liszka, 2007). Since this vest has no direct contact with human skin, it will allow patients to continue normal lives with a long-term telecardiology without any skin damage. A prototype of a biosensor shirt employs an R-peak detection algorithm, which can efficiently measure QRS complexes to detect cardiac anomalies such as bradycardia, tachycardia and sinus arrest (Pan and Tompkins, 1985; Liszka, 2007).

7 Research issues

In this section, we list some research issues. We do not intend to be comprehensive.

7.1 Data transfer issue

Regarding data transfer, there are two ways for data (e.g. images, audio or vital data files) to be sent to base stations: the store-and-forward (asynchronous) and real-time (synchronous) methods (Adler, 2000). In the store-and-forward method, data will be locally sampled by medical practitioners and sent to base stations in compressed forms. For example in the USA, about 30% of teledermatology examinations were performed in the store-and-forward method (Krupinski et al., 1999). Obviously, a problem of the store-and-forward method is overhead when data are compressed.

On the other hand, in the real-time method, doctors are able to see the health conditions of patients from direct raw data transferred in real time. Apparently, in the real-time method, overhead produced by data compression is reduced, which results in fresh captured data. There are also the following advantages: it enables doctors to conduct interviews with patients while watching images, and it enables them to advise practitioners as to how to capture physiological data. This method apparently improves the diagnoses of doctors. As a result, they can make quick decisions. In the field of telepsychiatry, roughly 20% of examinations in the USA, employs the real-time method (Krupinski et al., 1999).

However, despite the significant advantages above, the real-time method still has some problems. For example doctors in rural areas do not usually have enough time to see as many patients and practitioners as they walk-in, and therefore they hardly find time to see patients from telemedicine facilities (Adler, 2000). In most cases, a doctor should be in charge of patients from more than one facility. In other words, taking care of patients from telemedicine facilities may increase the physical burden on doctors. Regarding turnaround time, it often takes patients more time to receive diagnoses, since they first made their appointment to a hospital. This is because in the real-time method, patients expect to wait an extra time for their assignment to a doctor's busy schedule. Obviously, this extra time is not expected in the store-and-forward method. It turns out that the time spent on a patient assignment is a large difference between the real-time and store-and-forward methods, while the actual examination is of little difference, as it is 10–20 minutes for the real-time method and 5–10 minutes for the store-and-forward method (Adler, 2000). From research at the University of Arizona, 180 more hours are taken by the real-time method than the store-and-forward method to conclude diagnoses (Bashshur et al., 1997; Krupinski et al., 1999). Therefore, in the real-time method, doctors cannot afford to see walk-ins. Moreover, the real-time method requires higher resolution video conferencing equipment, which is usually expensive and requires more bandwidth. This kind of equipment may rarely be brought to patient houses. In other words, patients are required to commute to a nearby telemedicine facility to have a distant medical consultation. On the other hand, when using the store-and-forward method, captured physiological data could be temporally stored in a practitioner's PC and transferred to a doctor in his or her spare time. In this situation, practitioners could take a portable telemedicine kit with them to a patient's house. These days, even laptop PCs have supplied ample storage space for a reasonable price.

One concern about the store-and-forward method is that a failure to collect sufficient physiological data by practitioners requires another visit to patients. Once a practitioner is ready to transfer data at his or her office but is notified of a lack of data, he or she needs to take another trip to the patient. To avoid this inconvenience, careful discussion between a doctor and practitioners about data capturing before visits is necessary. Providing practitioner's manuals may help it be done properly. To the contrary, this situation becomes less of an issue in the real-time method. In this method, doctors are able to join the data capturing process with asking practitioners for physiological data needed for diagnoses. It largely reduces failure in the capturing process (Adler, 2000). More often than not, patients will be relieved more by having interviews with a doctor and hearing their direct comments about the symptom than only seeing a local practitioner. Furthermore, practitioners can also learn the latest medical techniques directly from doctors though the telemedicine sessions (Bashshur et al., 1997).

Therefore, it is hardly determined which method is more beneficial. Ideally, doctors should utilise the right method for the situation if they can afford to. In other words, a doctor should quickly see a patient through a video conference system (real-time method) when he or she determines that medical consultation is difficult without direct interviews. Otherwise, it may be sufficient for a local practitioner to take images of the diseased part and forward them in a compressed form to a doctor at a later time.

7.1.1 Quality of audio recording

In order to prevent aliasing, Nyquist sampling is used for the audio data. According to Nyquist, at least a double of the highest frequency is required for digital sampling to restore its original (analogue) raw data (Proakis and Salehi, 1994). For instance, since the frequency range of the heart and lungs is within 20 Hz to 2 KHz, a sound device that

captures these sounds should afford at least 4 KHz of sound frequency. Accordingly, a slight difference of frequency in the two sounds makes a large difference in the required bytes of the Nyquist. In practice, sampling a 10 second raw (16 bits per sample) mono audio at 8 KHz requires 83 kilobytes of memory space, whereas 44.1 KHz raw audio requires 390 kilobytes of memory space (Adler, 2000). So 128 kbps, the higher rate data transfer in the internet, makes it possible to transmit intact audio data in the store-and forward fashion (asynchronous). This 128 kbps transfer rate (8 KHz for 16 bit mono) is enough to restore the full human auditory frequency (20 Hz to 20 KHz) (Adler, 2000). Currently, even WLAN, such as Wi-Fi (IEEE 802.11g), implements up to 54 Kbps net bit rate.

7.1.2 Quality of image and video

The quality of the images sent to doctors is a very important issue in telemedicine because there is apparently a trade-off between the image quality and the size of the data (the speed of the data transfer). The higher the image quality, the slower the transfer of all data is. However, some examinations require high-resolution picture and video images. In fact, the image and video qualities are determined by each medical case because the quality required for remote medical consultation is different from one application to another. In other words, some applications may need high-quality resolution with a low frame rate, but other applications may require standard resolution with a high frame rate (Adler, 2000). For example a 200 × 200 pixels, 8 bit greyscale intensity resolution can fulfil the requirement of successful diagnoses for rashes on a human's hand. In a study by the University of Arizona research group on teledermatology, 83% of this kind of remote examinations can deliver the same quality as a face-to-face examination at a hospital. Likewise, a 256 × 256 pixels, 8 bit greyscale helps doctors successfully deliver correct diagnoses when examining digital Computed Tomography (CT) scan images (Bashshur et al., 1997). On the other hand, examining digital chest X-ray images requires much higher resolution (2000 × 2000 pixels, 12 bit dynamic range) (Adler, 2000).

Meanwhile, the Digital Imaging and Communication in Medicine (DICOM) committee is standardising a digital image transfer method and quality in the medical field ([DICOM is a joint committee of the American College of Radiology (ACR) and the National Equipment Manufacturers Association (NEMA)] (Pattichis et al., 2002). For use in remote medical examinations, DICOM recommends compression techniques that have been developed by ISO/IEC JTC 1/SC 29/WG 1, such as lossless JPEG, JPEG-LS and JPEG 2000 instead of originally developed compression schemes. Therefore, these compression techniques are very common in telemedicine (DICOM, 2010). To incorporate the standard into the current video compression system, Rao et al. (2009) proposed an Region of Interest (ROI) based elastic video coding system based on feedback from physician experts. This design is quite useful for delivering real-time diagnosis quality video in emergency cases. According to the experimental result, it indeed has diagnostically lossless (DL) quality within the ROI of the video. However, the ROI needs to be selected manually prior to the diagnosis, which may become an automatic process in future work.

7.2 Information security

In the age of wireless networks, people worry greatly about disclosure of their privacy to others, especially in the medical field. Concerning their worries, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the privacy protection standard, especially from the disclosure of the PCR (Hu et al., 2006a; US HHS, 2002). While HIPAA recommends populating the electric transaction for the field, it also provides a new safeguard for protecting the PCRs. In short, the PCRs, especially cardiac records, must not be exposed to a third party, but only sent to certain medical organisations or authenticated personnel without interceptions (Hu et al., 2006a).

At first glance, wireless networking potentially includes security risks because data transmitted through the air is rather easily captured by others. However, even in this situation, information concerning patient privacy must be carefully protected in such a way that these security issues will be concerned with both the physical (PHY) and MAC layers (jamming) (Mišić and Mišić, 2007). Basically, since it is in the WLAN, transmitted data will be strongly encrypted at end points. These encrypted data will not be decrypted easily by external malice in the middle of the transmission (Hackney, 2005). However, because of the limitation on computational power, the mote-based sensors cannot employ the traditional security and encryption techniques (Malan et al., 2004). Thus, in this case, encryption and security protocols must be lightweight and preferably low-power consuming. Moreover, some cardiologists suggest that encrypting ECG data will occasionally waste precious minutes required to save a patient from a heart attack (Liszka et al., 2004a).

There are many security aspects that can be applied to telemedicine. The following gives some examples: General security (Chen and Guizani, 2007; Michail et al., 2007; Mu et al., 2007; Memon and Goel, 2008; Mayrhofer et al., 2009; Yang, 2010; Wang and Jia, 2010), access control (Li et al., 2007), privacy (Sakarindr and Ansari, 2007; Zhu et al., 2007; Asadpour et al., 2008; Cronin et al., 2008; Tripathy and Nandi, 2008; Tsai et al., 2010), WiFi security (Malaney, 2007; Lin et al., 2008; Suomalainen et al., 2009), security in ad hoc or multiple hop networks (Gu et al., 2007; Hoeper and Gong, 2007; Hsu et al., 2007; Huang, 2007; Sun and Shayman, 2007; Ray and Poolsappasit, 2008; Djenouri et al., 2009; Wu et al., 2009; Xu et al., 2010), cache security (Erdogan and Cao, 2007), overlay security (Chen and Ji, 2007; Rabinovich and Simon, 2007), IP traceback (Korkmaz et al., 2007; Pan et al., 2007; Kotzanikolaou et al., 2008), key management in WSNs (Cheng and Chen, 2007; Ling and Znati, 2007; Srinivasan et al., 2008; Ma and Cheng, 2010), signature detection (Artan and Chao, 2007), authentication (Abdalla et al. 2007; Tartary and Wang, 2007; Laur and Pasini, 2009; Lee and Sivalingam 2009; McCune et al. 2009; Scannell et al. 2009; Huang et al., 2010; Li et al., 2007; Yang et al., 2010), secure aggregation (Bhaskar et al., 2007), security in sensor networks (Finnigin et al., 2007; Oliveira et al., 2007; Li et al., 2008a; Li et al., 2008b; Ma et al., 2008; Wang et al., 2008; Hsiao and Hwang, 2010; Richard et al. 2010; Soriente et al., 2009; Wang and Smith, 2010), secure conference (Zou and Karandikar, 2008), secure test beds (Hu et al., 2008a; Hu et al., 2008b; Hu et al., 2008c), security in

SCADA (Kilpatrick et al., 2008), intrusion detection (Bouhoula et al., 2008; Scheirer and Chuah, 2008; Uphoff and Wong, 2008; Ehlert et al., 2009; Dong et al., 2010), worm spreading (Burt et al., 2008; Chen et al., 2009), email security (Okolica et al., 2008), security in mesh networks (Kandikattu and Jacob, 2008), biometric security (Sadowitz et al., 2008; Buhan et al., 2009), secure services (Hsieh et al., 2008; Xu et al. 2008; Goodrich et al., 2009; Kuo et al., 2009), attacks and countermeasures (Berthier and Cukier, 2009; Hu et al., 2009a; Hu et al., 2009b; Hu et al., 2009c; Watkins et al., 2009; Malliga and Tamilarasi, 2010), security in satellite communication networks (Drakakis et al., 2009), key management (Challal et al., 2008; Bai and Zou, 2009; Bettahar et al., 2009; Chakrabarti et al., 2009; Guo et al., 2010), forensics and digital evidence (Rekhis and Boudriga, 2009), security in heterogeneous systems (Huang and Shieh, 2009) and RFID security (Palatini, 1999; Schwartz, 1999; Chobanian et al., 2003; Ma and Cheng, 2008; Azevedo and Ferreira, 2010; Dalton et al., 2010; Guo and Perreau, 2010; Hutter et al., 2010; Imasaki et al., 2010; Leng et al., 2010; Mahinderjit-Singh and Li, 2010; Raad, 2010; Rodrigues and James, 2010; Sun, 2010; Zhang et al., 2010).

7.2.1 Security policies

Before establishing the encryption models, security policies, such as what must be done and must not be done with the PCR, should be defined to secure the confidentiality and integrity of PCRs in the medical information system (Mišić and Mišić, 2007).

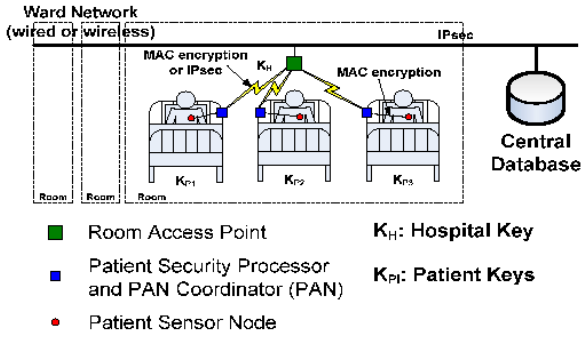
First, PCRs should be access-controlled such that only limited personnel can observe and modify the PCRs, and access control lists associated with the patients should be created in the system. The lists can present who and what clinician group can access the PCRs, and the system will restrict access to the PCRs according to the lists. Second, only the responsible clinician can maintain the access lists so that only he/she can add or delete PCRs on the lists. Thus, exactly one clinician (an administrator) is responsible for the lists (Mišić and Mišić, 2007). Every modification of the lists must also be reported to the patients so that those added to and deleted from the lists must be reported to the corresponding patients every time. Finally, the accountability of the PCRs must be established so that who, when and how authenticated staffs access the PCRs can be audited and, if necessary, reported to the corresponding patients.

In addition to confidentiality, in order to maintain the integrity of the PCR, data access should only be performed according to the following rules: creation, correction, deletion, confinement, aggregation and enforcement (Mišić and Mišić 2007). In the rule of creation, a new PCR should be accessed by the creator and the patient. The creation of a new medical record is therefore limited to the actual use only. The rule of correction demands that wrong information be modified, but old information must not be deleted for the sake of accountability. The deletion of data is performed only when the data expires. The rule of confinement states that appending one medical data to another can be performed only when the access control list of the second data is a subset of the first one. The aggregation rule restricts the aggregation of the PCR. Finally, the rule of enforcement states that all of the subsystems must be subject to the computer system that deals with the PCRs by following the aforementioned rules of integrity.

7.2.2 Security between wearable sensor nodes and personal servers

Since communication among the wearable sensor nodes and the PAN coordinator, or the PS, basically relies on the IEEE 802.15.1 or IEEE 802.15.4 in the WWBAN architecture, shown in Figure 18, one way to secure this portion of communication in wireless telemedicine is to use the security services specified by these standards (Mišić et al., 2007). For example the IEEE 802.15.4 provides useful security suites, such as access control lists, data encryption using pre-stored key, a message integrity code and message freshness protection. However, it is not enough to provide all of the security services to be required in this architecture. For example the IEEE 802.15.4 does not define the key management procedures, device authentication and freshness protection. These security services should therefore be complemented by the application layer. An example would be the ZigBee security API providing both the symmetric and asymmetric key exchange protocols (Mišić et al., 2007).

Figure 18 Architecture for healthcare wireless sensor networks (see online version for colours)



Source: Rosenbaum et al. (1996)

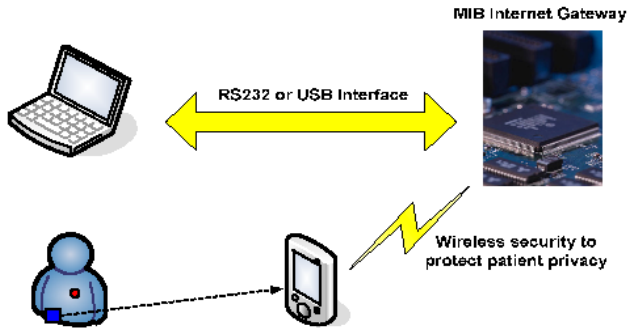
The ZigBee defines a Symmetric-Key Key Establishment (SKKE) protocol, which is based on the Keyed-Hash Message Authentication Code (HMAC) (Mišić et al., 2007). In this protocol, the secret keys (Link Keys) are shared by the sensor nodes and the PAN coordinator. The HMAC is calculated by a hash function with these shared secret keys. The ZigBee symmetric key exchange encrypts messages by the modified AES block cipher with 128 bits block size (Menezes et al., 1997).

The SKKE protocol will be established among the PAN coordinator and sensor nodes. At first, the PAN coordinator (denoted U) will generate and transmit the challenge QEU to the sensor node (denoted V). After validating the challenge QEU, node V will send back its own challenge QEV to the PAN coordinator. When the PAN coordinator receives and validates the challenge QEV, a shared secret key between these two devices will be generated by trustful steps (Mišić et al., 2007). However, the key updates still have some issues. For example when a key is updated, it will require synchronisation among the PAN coordinator and every sensor node in the cluster (Mišić et al., 2007).

7.2.3 Security between personal server and internet gateway involving multi-hopping

Like the CodeBlue architecture, some ad hoc sensor networks involve the multi-hopping scheme, in which the sensor nodes establish routes to relay data to the particular destinations (Malan et al., 2004). On one hand, the multi-hopping ad hoc sensor benefits entire energy consumption because sensors can keep a long distance data transmission by replacing it with multiple short distance hops (Hu et al., 2006a). On the other hand, in the context of security, employing the multi-hopping scheme in the wireless networks is still a challenging theme in the wireless network (Hu et al., 2006a). So, instead of a couple of PSs running on PDAs being involved in the route establishment, in one example of the security algorithms, a set of the PSs will be broken down into a number of subsets, namely 'clusters', and each cluster will have exactly one coordinator, namely a cluster head (CH), such that every member of the cluster can send the patient's vital data to the CH with only one hop (Hu et al., 2006a). A security protocol among clusters (cluster–cluster) employs the SkipJack security protocol to generate the intra-cluster session-keys (SK) during communications (see Hu et al., 2006a). In this example, both the PS and the Internet Gateway Devices [the Mote Interface Boards (MIB)] install the security software, as shown in Figure 19.

Figure 19 Security architecture (see online version for colours)

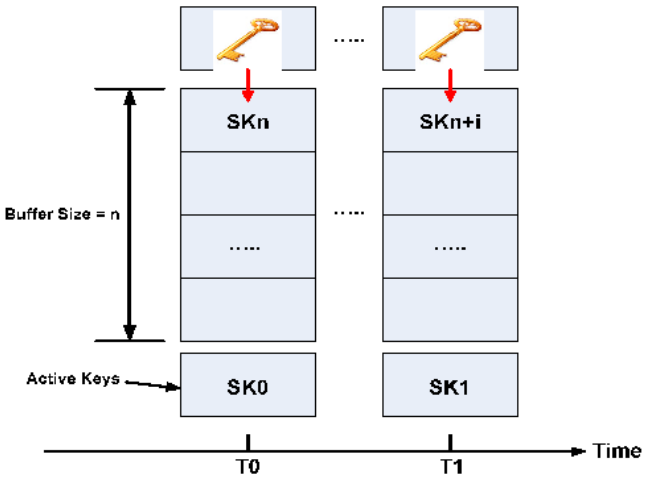


Source: Hu et al. (2006a)

In designing a security algorithm, there are two points to be considered: since the medical sensor networks usually deal with a few varieties of messages, a number of encryption patterns will be necessary to mask actual messages; because of the limitation on computational power and memory storage, a lightweight, low-power consuming algorithm will be appropriately chosen. To address these objectives, the initialisation vectors (IV) and the block cipher technique will be employed. In the use of the initialisation vectors, encrypting two same plain texts will be differentiated each time, and, in the block cipher technique, each message will be divided into several blocks to be encrypted as a unit (Brown, 1996).

Before the security session begins, each MIB obtains a long sequence of SKs that use a one-way hash function H(*) (e.g. $\{SK_M, SK_{M-1}, \ldots, SK_n, SK_{n-1}, \ldots, SK_0\}$ (size $M >> n$), as shown in Figure 20 (Hu et al., 2006a), where SKi = $H(SK_{i+1})$, and, among these SKs, only SK_n is broadcast to all CHs, which then calculate a sequence of SKs (e.g. SK_{n-1}, …, SK_0) for themselves from H(*)(Hu et al., 2006a). During a session, the encryption and decryption will first use SK_0, then SK_2, SK_3 and so forth. SKs that are not currently used (e.g. SK_n, …, SK_1) are preserved in a local key buffer (Hu et al., 2006a). At the same time, the MIB broadcasts new SKs from SK_{n+1} to SK_M to all the clusters at a fixed interval (Hu et al., 2006a).

Figure 20 Keychain-based security (see online version for colours)



Source: Hu et al. (2006a)

Now suppose a CH initially has n SKs such as SK_i, SK_{i-1}, …, SK_{i-n+1}, and it receives a new key SK_j at any moment, then the authentication will fail if the condition of this SK_j is (Hu et al., 2006a):

$$H\left(H\left(H\ldots\left(H\left(SK_j\right)\right)\right)\right) \notin \left\{SK_i, SK_{i-1}, \ldots, SK_{i-n+1}\right\}$$

Otherwise, the authentication is successful, and this SK_j will be temporally reserved to calculate (Hu et al., 2006a):

$$SK' = H\left(H\left(H\left(\ldots H\left(SK_j\right)\right)\right)\right), \text{ and } H\left(SK'\right) = SK_i .$$

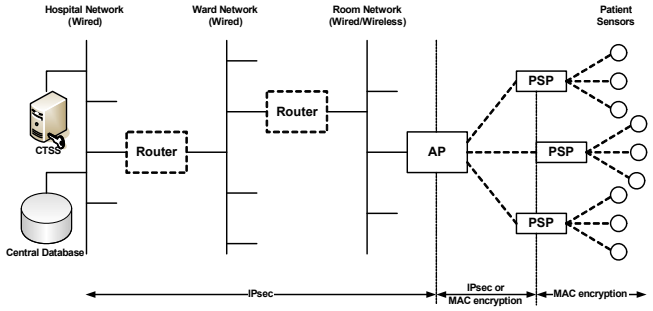
The calculated SK′ will then be pushed into the key buffer, and the other SKs will be shifted one position. At this point, one SK is presented and this SK is the current SK.

7.2.4 Security involving Central Trusted Security Server (CTSS)

Another security protocol runs the CTSS along with the central medical database (DB) (Mišić and Mišić, 2007). The CTSS manages the security protocols among devices. Other applications in the system must be subject to the security policies defined by the CTSS. Upon communicating data, devices in each group will share the symmetric encryption keys provided by the CTSS. In storing medical records into the DB, the CTSS will also make encryption and put the time-stamps on them. In patients' rooms, the Patient Security Processors (PSP), or the PSs, provide the private symmetric keys to all of the sensor nodes within the group by using the public symmetric keys provided by the CTSS. The PSPs are organised by the patient room access point that is also the gateway to the hospital networks (Mišić and Mišić, 2007).

Since the three-layer-tree-structured network architecture, as shown in Figure 21 (Turner, 2000), is hierarchical, it is better to employ the different keys and different encryption protocols to each layer and to use them according to the data importance and vulnerability, as well as the resource capacities, such as hardware memory.

Figure 21 Hierarchical structured architecture for healthcare wireless sensor networks



Source: Turner (2000)

The key is used for the signature and authentication of packets in the networks. According to the symmetric key, the vital data to be sampled, and the time-stamp, a packet authentication code will be calculated by using a hash function and the Security Hash Algorithm (SHA) (Mišić and Mišić 2007). Upon encrypting and decrypting the PCRs, the private patient keys, e.g. Kp, are applied to compute the encryption and decryption functions, such as EKp( ) and DKp( ), respectively (Mišić and Mišić, 2007). These keys are shared only by a certain group of people that includes the patient, the responsible (principal) clinician and the referring clinician. So, in practice, at least three people, including the patient, are required to generate and share a patient key, and only the people participating in the key generation can share the key. Moreover, one generation of the key is only available in one session where members of the access control list are still unchanged. As long as a predefined period of time has not been expired, the session will continue. In short, the keys are only usable among particular people within a particular period of time. The key generating process is explained by Mišić and Mišić (2007).

7.3 Routing challenges of WBAN telemedicine in MANET

In the case of mass casualty situations, upon updating the victims' physiological conditions, always multicasting (pushing) data to all of the client devices will waste network bandwidth because there will be a number of sensors sampling and transmitting data. These low-power sensor nodes are usually limited to their network bandwidth. Moreover, all of the client devices are not required to see all of the data from every sensor node. To avoid this redundancy, only devices that are interested in that data should request the data. Since connection channels will only be established between these devices, this framework will reduce network redundancy.

CodeBlue employs a publish/subscribe routing framework based on ADMR (Malan et al., 2004; Shnayder et al., 2005). In this process, when one sensor node is ready to publish data, it first multicasts only a request to publish to all of the neighbouring nodes. Upon receiving, these nodes will again multicast the data to relay it to all of the local client devices (multi-hopping). After it reaches all of the client devices, if some of them need to subscribe the data, they send a subscribe request to the publisher. In the returning process, the subscribe request will establish the routes from the publisher to the subscribers. By using these routes which are assigned to particular channels, communication between the publishers and the subscribers will be achieved. Basically the publishing data include the physiological data, location and client device identity (Malan et al., 2004). Moreover, a 15 seconds update period of CodeBlue will maintain the routings from changes in network topology by node movement (Shnayder et al., 2005).

7.3.1 Adaptive Demand-driven Multicast Routing (ADMR)

In the route discovery protocol of the ADMR, every node has a node table which contains the publisher node ID, path cost and previous hop. The path cost is the number of transits made before arriving at the node from the publisher. When the publisher makes a request for publishing information, it simply multicasts the publish request message (ROUTE-DISCOVERY) to the neighbour nodes. Every time that ROUTE-DISCOVERY arrives, each node makes a comparison between the node table entry and the coming estimated path cost. If this path cost is smaller than the old table entry, the node table is modified (Shnayder et al., 2005; Chen et al., 2006). So, when receiving nodes get ROUTE-DISCOVERY, they will also have the smallest path cost and previous hop in the node table, and consequently every node can establish the shortest path from the publisher to itself (Shnayder et al., 2005).

The receiving nodes which want to subscribe the information send the subscribe request message (RECEIVER-JOIN) to the previous node according to the previous hop in the node table. This message is passed through the entire path in the opposite direction towards the publisher (Shnayder et al., 2005). During transmission, every node which relays RECEIVE-JOIN turns into a forwarder for the requested channel (Shnayder et al., 2005). In order to mitigate the loss of RECEIVER-JOIN, the hop-by-hop acknowledgement is employed (Shnayder et al., 2005). To accommodate any network topology due to node movements, periodical updates of the node tables are also required (Shnayder et al., 2005). Although the ADMR is designed to optimise route construction, it sometimes leads to congested paths (De Couto et al., 2003; Woo et al., 2003).

This route discovery algorithm is important because the route selection metrics inevitably affect the performance of the communication (Chen et al., 2006). Moreover, since the forwarders never know who is the sender and who is the receiver, and they just broadcast messages to the neighbour nodes, some nodes can receive the same message multiple times. To avoid this situation, the forwarders will log the received messages and never forward the same messages twice but just omit them (Chen et al., 2006).

For these several reasons, forwarders no longer required to be forwarders. For example the receiver movements cause some forwarders to be taken away from the route (Chen et al., 2006). Also, when the receiver no longer has interest in particular information, the forwarders establishing the route should be dropped in order to save bandwidth (Chen et al., 2006). To achieve the state expiration, passive acknowledgement is used in the ADMR.

The node table entry has the lifetime to prompt route pruning and avoid wasting bandwidth (Chen et al., 2006). According to the path reinforcement policies, the lifetime of the node table entries is either preserved or expired (Chen et al., 2006). The refreshment of the lifetime follows two policies: active reinforcement and passive reinforcement. In active reinforcement, forwarders can refresh their lifetimes as a new RECEIVER-JOIN arrives. On the other hand, in passive reinforcement, the passive acknowledgement survives the forwarder membership (Chen et al., 2006).

7.3.2 PATH-DR protocol

Although the original ADMR intends to minimise the hop count (MIN-HOP), this protocol may be attempted to choose the shortest path with the very noisy radio link (Chen et al., 2006). This protocol is also often problematic if the nodes have mobility, i.e. the radio link quality between the nodes is unstable (Chen et al., 2006). ADMR always chooses routes with the robust radio link. CodeBlue employs the PATH-DR protocol, which intends to maximise the total Path Delivery Ratio (PDR) (Shnayder et al., 2005; Chen et al., 2006). In practice, the total PDR is a metric to represent the total robustness of the radio links along the routes from the publisher to the subscriber. The best PDR is therefore derived from the aggregation of the hop-by-hop Link Delivery Ratio (LDR), which is the robustness of the radio link between two nodes. However, since detecting out the LDRs requires neighbouring nodes to exchange multiple massages, this will cause messaging overhead. Thus, instead of directly applying the LDR as a route estimator, the Harvard University research group applied the CC2420 radio's Link Quality Indicator (LQI) to the route discovery because it was found that there is a correlation between the LDR and the CC2420 radio's LQI (Shnayder et al., 2005; Chen et al., 2006). The CC2420 can generate the LQI with a single packet exchange. Hence, the PATH-DR is simply calculated by maximising all of the products of the LQIs along the route from the publisher to the subscriber (Chen et al., 2006).

7.3.3 Scalability

Scalability of the ad hoc sensor networks is mainly considered in the next three points: data rate scalability, sender device scalability and receiver device scalability. For example data rate scalability can be affected when the number of hop counts of a route increases. As the number of hop counts increases, some nodes may be assigned to become forwarding nodes of the different senders, and the data traffic of these nodes will be congested. Likewise, the sender and receiver device scalability will affect how many sender or receiver devices are allowed to work in the networks.

In the context of data rate scalability, when doctors or nurses are comparatively close to the patients, only the single-hop data transmission will be required for data to get to the doctor's or nurse's personal server from the patient's sensor nodes. In single-hopping, since the pier-to-pier connection can be established between the doctor's and the patient's sensor nodes, the average reception rate will be stably high for the high data transmission rates because the data traffic is hardly congested (Shnayder et al., 2005). However, as the number of hop counts from the sensors to the personal server increase, the average reception rate will fall below 40% in the case of 50 packets per second (Shnayder et al., 2005). This is because the forwarding nodes between the senders and the receivers cannot have enough bandwidth to deal with both the upstream and downstream data transmission as the data transmission rate increases. So when the packet queue is filled up, the incoming packets will be simply ignored (Shnayder et al., 2005). Traffic data collisions between the upstream and downstream will also degrade the average reception rate sensitively (Shnayder et al., 2005).

Likewise, as the sender nodes increase, the hop counts increase (Shnayder et al., 2005). However, in suppressing the data transmission rate such that each sender sent below 5 packets per second, the average reception ratio was kept above 62% in experiments (Shnayder et al., 2005). So, if the amount of data rate is suppressed below once per second, the number of sender nodes would be largely scalable (Shnayder et al., 2005).

In the experiment in which three receiver nodes receive messages from different numbers of sender nodes of a different data rate, even if only a single sender transmits messages, multiple hops will occur (Shnayder et al., 2005). The data rate inflation would therefore inevitably affect the quality of the data transfer. From the results of these experiments, 10 sender nodes with 10 packets per second degraded the average reception ratio to nearly 40% (Shnayder et al., 2005). Moreover, this value was very close to a single sender unicasting messages with 30 packets per second (Shnayder et al., 2005).

7.3.4 Mobility

Experiments to measure the impact of the movements of nodes were conducted by the Harvard University research group such that the receiver nodes would be roaming like a human walking, which would include pausing and entering and leaving rooms (Shnayder et al., 2005). These experiments involved three senders and a receiver at five packets per second. The measurements were performed over 60 second intervals and the average was calculated (Shnayder et al., 2005). Although the average reception ratio varied, any critical degradation did not emerge in the experiments (Shnayder et al., 2005).

One major issue regarding mobility is BSN application. Since sensor nodes only have limited power and communication range, continual movement of patients may lower the precision of sensing. To overcome this problem, two on-going research topics are considered. One is host mobility (Chiti et al., 2009), which helps to track and locate patients. Another related technology is known as context awareness (Chiti et al., 2009), which can extract useful surrounding information to benefit the efficiency of the mobile BSN. For the purpose of saving energy and establishing a better power management in the mobile BSN, Chiti et al. (2009) proposed a context aware BSN framework for patient monitoring. This work enables a mobile BSN to dynamically join a nearby WSN by using a context aware monitoring paradigm (Chiti et al., 2009). So based on the location of the WSN hotpot, patients with such a mobile BSN may be traced. Authors also designed a novel MAC layer communication protocol, known as MD-STAR. It improves the capabilities of wireless communication between mobile BSN and fixed WSN (Chiti et al., 2009). The main advantage of MD-STAR is the low latency of re-establishment while hopping to the next WSN. Meanwhile, it also enhances the overall performance of the BSN system, especially regarding energy reduction (Chiti et al., 2009).

7.3.5 Fairness, latency and jitter

Fairness expresses whether choices of routes are evenly distributed throughout the networks. To seek the fairness of the ADMR, the Harvard University research group measured the average reception ratio of the case of six senders and three receivers with a maximum of six hops (Shnayder et al., 2005). For example the average reception ratio of the pair of sender 1 and receiver 1 was over 70%. According to the bar graphs, shown in Figure 21 (Turner, 2000), almost all of the reception ratios were fairly distributed but that of sender 6 and receiver 2, in which the average reception ratio was degraded to below 60% (Shnayder et al., 2005).

From the perspective of the latency of the ADMR, (see Shnayder et al., 2005), the experiments of the Harvard University research group concluded that the end-to-end data transfer latency would be less than 200 ms in the case of not more than seven hops per route (Shnayder et al., 2005).

Packet jitter is how many successive packets will be lost for a sender–receiver pair, and this can be counted by investigating how the transmitted sequence of numbers will be received by the receiver nodes (Shnayder et al., 2005). Results from the experiments of the Harvard University research group showed that, in nearly 70% of single sender–receiver pairs with an average of five hops per case, no packet jitter would appear, that one packet jitter would be recorded in 22% of cases, and that two or more packet jitters would be recorded totally in 8% of cases (Shnayder et al., 2005). On the other hand, in the multiple senders and receivers cases, experiments involved six senders and three receivers at the data rate of one packet per second in the sensor networks and were classified into multi-hop pairs, single-hop pairs and across all 18 pairs. According to Shnayder et al. (2005), in 86% of cases, no packet jitter would appear, in 9% of cases, one packet jitter would be recorded, and two or more jitters would be recorded in 5% of cases. Not more than 23 packet jitters would be recorded in the experiment (Shnayder et al., 2005). From the observation of the first pair nodes, the Harvard University research group concluded that, in the multiple senders and receivers cases, the increase of the number of forwarders can suppress the increase of the number of jitters.

7.3.6 Packet loss

To achieve mitigation of packet loss, multiple data transmission is performed. Although this approach improves the probability of the receiver nodes getting the packets in some degree, the network saturation caused by the low bandwidth must be taken into account, as well as the average reception ratio of the redundant data transmissions. The experiment was conducted in the cases of a single sender–receiver transmission with an average of five hops (Shnayder et al., 2005).

Compared with 1-transmit (where the average reception ratio was 63%), the average reception ratio of 5-transmit was clearly improved to above 98% for the low-data rate (Shnayder et al., 2005). However, as the data transmission rate increased, the network robustness was considerably degraded and eventually dropped under the line of the 1-transmit case (Shnayder et al., 2005). This is because more data transmissions will inevitably require more bandwidth, or otherwise network saturation will eventually emerge (Shnayder et al., 2005).

7.4 Routing challenges in embedded biomedical sensor networks

Another application of telemedicine with the WWBAN architecture is to directly implant the biomedical sensors in the human bodies. This kind of biomedical sensor is called an in vivo sensor. Like the basic wearable vital sensors, the in vivo sensors can sample biometric data and transmit it to the practitioner's terminals using the WSNs (Furse et al., 1999; Schwiebert et al., 2001; Furse et al., 2002; Schwiebert et al., 2002; Bag and Bassiouni, 2006). So these sensors are considerably applicable to artificial retina, the glucose level, organ monitoring and cancer detecting (Schwiebert et al., 2001).

However, implanting sensors into the human body will cause another issue within the telemedicine technology. Since the in vivo sensors usually continue transmitting biomedical data to the outside sensor nodes, heat caused by processing and communication will emerge inside of the human body. Obviously, the rising temperature of the in vivo sensor nodes is dangerous for the surrounding tissues, and a high temperature may damage them in long-term monitoring (Schwiebert et al., 2002; Bag and Bassiouni, 2006). As implantable sensors, heating is not allowed to exceed 0.7 degrees in US legislation. Thus, regarding the in vivo sensor nodes, routing protocols should be designed to

avoid producing rising temperatures from the implanted nodes. That is data transmissions among the nodes should disperse around the communication and not focus on only one route (Bag and Bassiouni, 2006). In addition, for the sake of reducing exposure to IR radiation (a kind of electromagnetic radiation), consideration of the power consumption is also important. Because lower batteries require recharging by IR radiation, easily expending battery life should be required to recharge often, increased exposure the surrounding tissues to the IR radiation and should be avoided (Heinzelman et al., 2000; Shankar et al., 2001; Prakash et al., 2003; Tang et al., 2005). Of course, the latency of the network communication is also considered in critical situations.

To avoid heat generation, four TARAs are developed: TARA, Least Temperature Routing (LTR) protocol, Adaptive Least Temperature Routing (ALTR) protocol (Schwiebert et al., 2001) and Least Total-Route-Temperature (LTRT) protocol (Takahashi et al., 2008). We will explore these four TARAs in depth in the next subsections.

7.4.1 Thermal Aware Routing Algorithm (TARA)

The TARA is designed to solve these constraints. At first, the TARA defines a hotspot as an area where some nodes have high temperatures due to a focus on data communications (Bag and Bassiouni, 2006). Upon detecting the hotspots, to avoid producing rising temperatures of this area any longer, the TARA aims to establish other routes around the hotspots by using the withdrawal strategy (Bag and Bassiouni, 2006). In this strategy, upon receiving the packets, when the surrounding (neighbouring) nodes except for the sending node, are all hotspots, this node sends back a packet to the sender node and the sender node then selects a detour around the hotspots or sends it back to the previous node (Bag and Bassiouni, 2006). After cooling the temperature of the hotspots to below a predefined limit, the TARA takes these areas into consideration as candidates for later routing. To accomplish the TARA effectively, every node must know the temperature change of the neighbour nodes, i.e. which ones are hotspots. Thus, each should always monitor the neighbours' packet counts and calculate the communication radiation and power consumption to derive the current temperature of the neighbours. The hotspot, which exceeds the predefined minimum temperature limit, must be checked by the surrounding nodes, and later kept from participating in routing until its temperature is standardised. An example of TARA is shown in Figure 22.

7.4.2 Least Temperature Routing (LTR)

Like the TARA, the LTR protocol is designed to avoid establishing routes on hotspots in order to keep the temperature low in particular in vivo sensor nodes. However, unlike the TARA, the LTR always chooses the neighbour nodes which have the lowest temperature for routing (Bag and Bassiouni, 2006). So, unless the packets are sent to the particular neighbouring nodes which are their destination, the nodes always send the packets to their coolest neighbours (Bag and Bassiouni, 2006). The LTR also employs packet discarding for the sake of maintaining network bandwidth (Bag and Bassiouni, 2006). Each packet roaming the network maintains its hop-count by each hop. Compared with a predefined minimum hop-count, namely MAX_HOPS, if the value of the hop-count exceeds MAX_HOPS, the current sensor node will discard the packet from the network. In addition, to avoid infinitely looping the same route, the packet wandering in the network can maintain a table which keeps track of the nodes that the packet most recently passed through (Bag and Bassiouni, 2006). Thus, if the next node where the packet will be forwarded (coolest neighbour) is already on the table, the current node will pass the packet to the second lowest temperature node which is not on the table to avoid choosing the same route. This consequently prevents packets from infinitely looping the same route. An example of LTR is shown in Figure 23.

Figure 22 An example of Thermal Aware Routing Algorithm (TARA) (see online version for colours)

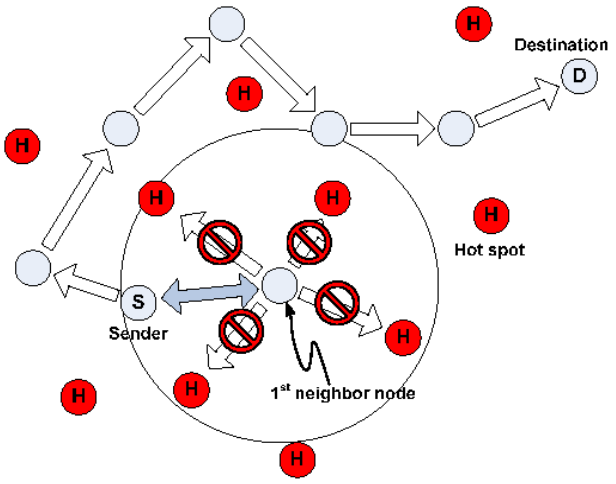
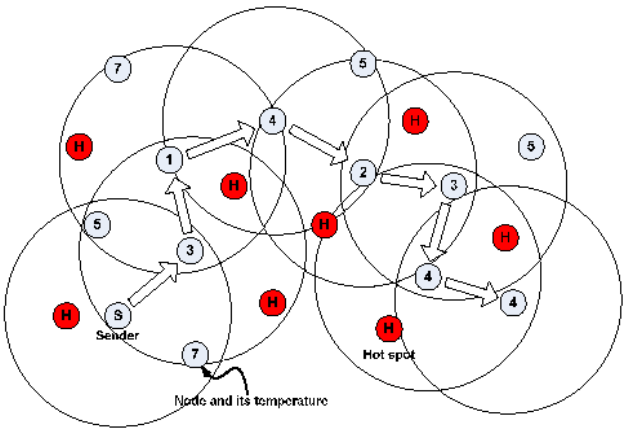


Figure 23 An example of LTR (see online version for colours)

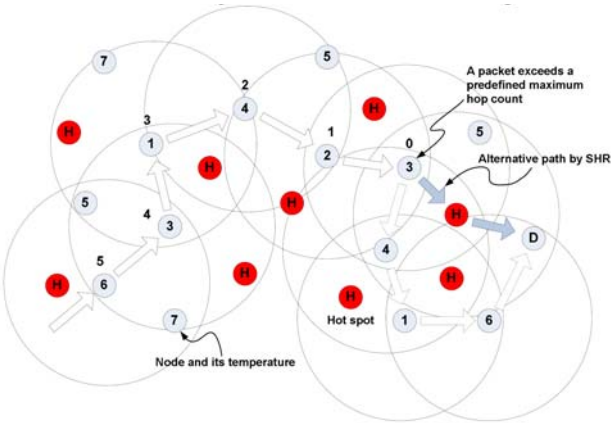


7.4.3 Adaptive Least Temperature Routing (ALTR)

One of variants of the LTR protocol is the ALTR protocol. The difference between the LTR and the ALTR is that, while the ALTR as in the LTR employs hop-count in the packets and

keeps track of the hop-count of each packet in every hop, when the value of the hop-count exceeds a predefined minimum hop-count, namely MAX_HOPS_ADAPTIVE, it can use the Shortest Hop Routing (SHR) protocol as an alternative protocol to take the packets to the destination as soon as possible (Bag and Bassiouni, 2006). The ALTR can adapt to particular topologies. Since in some network topologies, such as the ring topology, the packet sequence inevitably traces the same path and the temperature of nodes on the particular paths will get rapidly increase, the 'proactive delay' mechanism is utilised by the ALTR (Bag and Bassiouni, 2006). In this 'proactive delay' mechanism, upon getting a packet from some node, there are at most two ways to send the packet, but their temperatures are comparatively high. The current node can therefore wait a unit time before sending it to the coolest neighbour in order to lower their temperature (Bag and Bassiouni, 2006). Although the packet latency becomes somewhat higher, the average temperature of the network can decrease in this mechanism. An example of ALTR is shown in Figure 24.

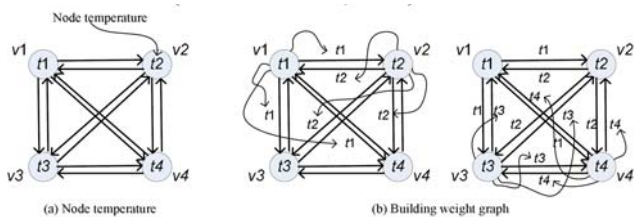
Figure 24 An example of ALTR (see online version for colours)



7.4.4 Least Total-Route-Temperature (LTRT)

Since none of the former three schemas accomplishes optimisation for routings, the LTRT protocol is designed to solve problems that cause the redundant hops and total temperature rise (Takahashi et al., 2008). The main idea of LTRT is to convert nodes' temperatures into graph weights and to then select a least possible temperature route from sender to destination. They do not always choose the least temperature sensor nodes. In short, LTRT calculates routes from the single source shortest path algorithms in graph theory (e.g. Dijkstra's algorithms) and applies these routes for later packet transmissions. Thus, like TARA, LTR and ALTR, LTRT requires every node to obtain the temperature of its neighbouring nodes from the received and transmitted packets (Takahashi et al., 2008). The protocol follows the next four steps: (a) assign the temperatures of sensor nodes as weight to each sensor node based on communication between neighbouring sensor nodes, as shown in Figure 25(a); (b) in calculating routes, transfer weight of sensor nodes to weight of edges ahead, as shown in Figure 25(b); (c) by using the second graph, apply single-source shortest path algorithms to figure out routes having the least temperature from sending nodes to destination; (d) to avoid excessively raising the temperatures of sensor nodes, periodic maintenance (updating) of routes is required, which also helps in adapting frequenting network topology changes caused by node movements. Detailed discussion and simulation results can be found (see Takahashi et al., 2008).

Figure 25 An example of LTRT) (see online version for colours)



Source: Takahashi et al. (2008

7.5 Telemedicine in future

As computer technology progresses, some advanced features will be integrated into telemedicine systems. The latest technology in the field of Artificial Intelligence (AI), data storages, compression and high-speed wireless communication, together with new non-invasive biological and medical sensors, now enables telemedicine systems to be the new generation (Adler, 2000). Both cost effective and multi-functional portable telemedicine kits with multiple languages will emerge in the near future (Adler, 2000). In this subsection, we describe the newest technology in each field, which should be augmented into the next generation of telemedicine kit, and later introduce a wireless home medical monitoring system.

7.5.1 Wireless communications of telemedicine

In addition to the connectivity of the wireless network, high-speed wireless protocols should also be considered. For example Bluetooth, which is an ad hoc style, achieves 1 Mbps at 2.5 GHz within a range of 10 metres, and HomeRF achieves 1.6 Mbps within a range of about 50 metres (Negus et al., 2000). It is a low-cost and well-developed technology for data transmission in wireless communication. Recently, researchers have studied such a telemonitoring system (Wang and Gu, 2009). Using Bluetooth, this device may monitor several significant physiological features remotely, such as heart rate, body temperature and blood pressure (Wang and Gu, 2009).

7.5.2 Artificial intelligence

Researchers will continue to build expert systems which help doctors and specialists make medical decisions based on incoming data (Bashshur et al., 1997). For example the expert system Mycin at Stanford University in the mid-1970s could already support specialists in diagnosing medical conditions 'as well as medical experts' (Buchanan and Shortliffe, 1984). Similarly, NASA also utilised expert

systems which could make medical decisions for astronauts in the space (Adler, 2000). Thus, in the near future, expert systems will accurately analyse audio-visual data and directly give patients or practitioners diagnoses instead of specialists.

7.5.3 Data compression technology

The rapid progress of computer power and memory storage will be able to empower data compression technology. Although lossy compression algorithms are capable of performing up to 10:1 ratio compression, they are still insufficiently for clinical needs (Bashshur et al., 1997). Advanced data compression is applied to mainly video data where fundamental image updates rarely occur in many cases (i.e. background images) (Adler, 2000). Moreover, abbreviating the uniform frame code should additionally reduce video data (Bauer and Ringel, 1999).

Hu et al. (2009c) has been proposed a congestion-aware, loss-resilient bio-monitoring system with data compression technology. This system, called PSoc, integrates WSN software and hardware platforms. Several commonly used appliances and technologies are involved, such as ECG, EEG, RFID and RF board (Hu et al., 2009c). To reduce the size of transmitted data, it compresses the delivering packages by only transmitting bio-signal feature parameters (Hu et al., 2009c). While receiving those packets, PSoc will use wavelet-based signal decomposition to retrieve the original signal. Since the recovery process is not 100% correct, Hu et al. (2009c) proposed ripple-based local recovery and an erasure-codes-based method to the receipt of each package.

Data compression methods also benefit the development of wireless telecardiology. Sufi et al. (2009) proposed a new ECG compression algorithm for the ECG signal's transmission over a limited bandwidth network (e.g. mobile phone platform). Through their approach, current mobile phone-based cardiovascular monitoring services will speed up to 6.72 times faster than previous solutions (Sufi et al., 2009). To facilitate our current telemedicine application, data compression technology should be further studied.

7.5.4 Medical sensors

In recent years, medical sensors like the GlucoWatch Biographer (manufactured by Cygnus, Inc., in Redwood City, CA), which checks blood sugar levels for diabetics without any pain, have achieved dramatic progress (Adler, 2000). Biosensors are, for example, used to interpret a couple of inputs, such as blood pressure, joint position or brain waves, electronically into digital signals (Bauer and Ringel, 1999). In addition, Cyranose (made by Cyrano Science in Pasadena, CA) is able to convert smell into electrical signals. Cyranose was a recently introduced, small, electrical nose which was capable of analysing chemical compounds not only from exhaled air but also from urine or body fluids, and from skin diseases or bacterial infections. These sensors reside with the telemedicine systems as alternatives.

7.5.5 Medical recorders

Although the uses of Electrical Medical Records (EMRs) are limited, they will be made available for research, education and medical practice in the future. EMRs are currently in need of universal standards and restrictions on accessing patients' records for themselves (Bauer and Ringel, 1999). No later, however, these restrictions will be removed, and patients and chosen practitioners will be able to retrieve the records from anywhere at any time (Bauer and Ringel, 1999). Then, constructing a public database of telemedicine diagnoses will be productive for practitioners, doctors and researchers, as well as patients (Adler, 2000).

7.5.6 Home health monitoring system

With wired or wirelessly networking houses, we will easily be able to put telemedicine devices into any place in the houses (Dutta-Roy, 1999). Along with the home networks, IP-enabling medical devices, through the use of a chip, such as Filament, will be able to realise in-home telemedicine systems (Adler, 2000). Then, various physiological parameters like blood pressure will be captured within the home. For instance, a toilette could discern signs of colon cancer or renal failure, and telephones and a hand shower could be equipped for sensing blood glucose and an ultrasound (Bashshur et al., 1997).

Jara et al. (2009) proposed an Ambient Assisted Living (AAL) system to support home healthcare. It integrates several fashion technologies and refers to European electronic health records. With the help of PDA, WBAN and ZigBee network technologies, this system is capable of remote connection and control (Jara et al., 2009). Based on those records, it also may utilise chronobiology algorithms to predict some illness or to detect some symptoms using a simple rule system (Jara et al., 2009). Taleb et al. (2009) designed a similar framework for assisting elders at home. It is named ANGELAH, which stands for '*AssistiNG ELders At Home*' (Taleb et al., 2009). The ANGELAH is also capable of elder monitoring and emergency detection. What makes it outstanding is the ability to create and manage volunteer rescue teams for emergency events. However, the privacy issue in ANGELAH needs to be further studied.

7.5.7 Wireless transduction from medical devices

To achieve the home health monitoring system, Adler (2000) developed a small transceiver board with wireless low bit transmission. A programmable chip (Microchip PIC16F873) and an 868 MHz RF transceiver chip (RF Monolithics DR3001), together with an RS-232 serial line driver (Maxim Integrated Circuit MAX233), are integrated on the transceiver board (Adler, 2000). The PIC has 12 digital I/O channels to pick up data from devices, and the transceiver chip then sends the data to the base station at 19.2 kbps (Adler, 2000). This same board is also used by the base station for receiving data transmissions and communicating with a PC (Adler, 2000).

Peripheral devices, such as a stethoscope, ECG, thermometer and scale can involve this board. They can also achieve transparency for users (Adler, 2000). In each measurement by a wireless medical device, the base station records remote data and sends it to a doctor on a regular basis (Adler, 2000). At this point, to accomplish mutual exclusion among the various devices, Adler (2000) developed a unique protocol:

1 When devices are ready to transmit data, they send a unique ID to the base station.

2 The base station picks up one of these IDs and stops other transmission.

3 After obtaining data correctly, the base station sends an acknowledgement to the device and stops it until the next use.

4 The base station transmits a signal to the other devices to begin their activity again.

A Java Applet is used to achieve this protocol, and this simple programme can also perform the information updates on a secured website (Adler, 2000).

Bluetooth, a high bandwidth wireless protocol, will possibly be able to be used to accomplish seamless data transmission from streaming audio devices, such as a stethoscope. It can easily be embedded into medical devices within a 10 metres range because of built-in serial, USB and audio connections (Adler, 2000).

8 Conclusion

This paper introduced some wireless technologies that can be used in telemedicine. We surveyed wireless telemedicine and m-health applications with examples. This paper briefly introduces the current state of telemedicine technology, applications and their problems. Although telemedicine technology initially started with the two-way remote medical consultations between the medical specialists, it is now applicable to mass casualty disasters and in vivo sensors. However, the more complex the telemedicine system becomes, the more sophisticated the techniques required to be implemented in the system will become. For example in the ad hoc medical sensor networks, to achieve the non-obtrusiveness of the medical sensors, the size of the motes was preferably decreased. But this miniature size also constrained the computational power and energy resources of the motes, which caused applied routing protocols and security algorithms to be inevitably lightweight and low-power consuming. Besides, the reliability of the network is also affected by the computational resources and energy consumption of the devices.

QoS is another issue in telemedicine technology. Data to be dealt with in telemedicine are sometimes critical to human life. The physiological as well as the audio-visual data must be clear enough for the remote doctors to make diagnoses in real time. Generally, higher qualities or resolutions of the audio-visual data require higher bandwidth and advanced data compression techniques. However, these advanced technologies require high computational power and energy consumption of the devices. These trade-offs must therefore be considered in the further researches.

At last, since the QoS of telemedicine usually varies case-by-case because the quality required for the remote diagnoses is different from one application to another, designing the telemedicine architecture should be scenario-based. For example in mass casualty disasters, system architectures like CodeBlue of the Harvard University will effectively solve many problems which cannot be solved by the other applications. To design the telemedicine architecture, we must consider what cases the telemedicine systems will be applied to.

Acknowledgements

This research is supported by the US National Science Foundation (NSF) under grant CNS-0716211. Any ideas presented in this paper do not necessarily represent NSF's opinions.

References

10BLADE (2004) *iRevive Feature List*. Available online at: http://www.10blade.com/irevive.html (accessed on 13 October 2010).

Abbes, T., Bouhoula, A. and Rusinowitch, M. (2010) 'Efficient decision tree for protocol analysis in intrusion detection', *International Journal of Security and Networks*, Vol. 5, No. 4, pp.220–235.

Abdalla, M., Bresson, E., Chevassut, O., Moller, B. and Pointcheval, D. (2007) 'Strong password-based authentication in TLS using the three-party group Diffie–Hellman protocol', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.284–296.

Abowd, G.D., Bobick, A.F., Essa, I.A., Mynatt, E.D. and Rogers, W.A. (2002, July) 'The aware home: a living laboratory for successful aging', *Proceedings of AAAI Workshop Automation as Caregiver*, Alberta, Canada, pp.1–7.

Adler, A.T. (2000) *A Cost-Effective Portable Telemedicine Kit for Use in Developing Countries*, Master of Science in Mechanical Engineering Thesis, MIT, USA.

Antoniades, C., Kouppis, A., Pavlopoulos, S., Kyriakou, E., Kyprianou, A., Andreou, A.S., Pattichis, C. and Schizas, C. (2000) 'A novel telemedicine system for the handling of emergency cases', *Proceedings of the 5th World Conference on Injury Prevention and Control, World Health Organization (WHO)*, New Delhi, India.

Artan, N. and Chao, H. (2007) 'Design and analysis of a multipacket signature detection system', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.122–136.

Asadpour, M., Sattarzadeh, B. and Movaghar, A. (2008) 'Anonymous authentication protocol for GSM networks', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.54–62.

Azevedo, S.G. and Ferreira, J.J. (2010) 'Radio frequency identification: a case study of healthcare organisations', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.147–155.

Baard, M. (2004) *RFID Keeps Track of Seniors*. Available online at: http://www.wired.com/medtech/health/news/2004/03/62723 (accessed on 13 October 2010).

Bag, A. and Bassiouni, M.A. (2006, October) 'Energy efficient thermal aware routing algorithms for embedded biomedical sensor networks', *2006 IEEE International Conference on Mobile Adhoc and Sensor Systems*, Vancouver, Canada, pp.604–609.

Bai, L. and Zou, X. (2009) 'A proactive secret sharing scheme in matrix projection method', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.201–209.

Bao, S.D. and Zhang, Y.T. (2005, September) 'Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems', *Proceedings of 27th IEEE International Conference of Engineering in Medicine and Biology Society*, Shanghai, China, pp.2455–2458.

Bao, S.D., Zhang, Y.T. and Shen, L.F. (2005, April) 'A new symmetric cryptosystem of body area sensor networks for telemedicine', *Proceedings of 6th Asian-Pacific Conference on Medical and Biological Engineering*, Japan.

Bashshur, R.L., Armstrong, P.A. and Youssef, Z.I. (1975) *Telemedicine: Explorations in the Use of Telecommunications in Health Care*, C.C. Thomas, Springfield, IL.

Bashshur, R.L., Sanders, J.H., Shannon, G.W. and Foundation, B. (1997) *Telemedicine: Theory and Practice*, C.C. Thomas Publishers, Springfield, IL.

Bauer, J. and Ringel, M. (1999) *Telemedicine and the Reinvention of Healthcare*, McGraw-Hill, New York.

Behrman, R.E. (2000) *Nelson Textbook of Pediatrics*, W.B. Saunders Company, Philadelphia, PA.

Berthier, R. and Cukier, M. (2009) 'An evaluation of connection characteristics for separating network attacks', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.110–124.

Bettahar, H., Alkubeily, M. and Bouabdallah, A. (2009) 'TKS: a transition key management scheme for secure application level multicast', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.210–222.

Bhaskar, R., Herranz, J. and Laguillaumie, F. (2007) 'Aggregate designated verifier signatures and application to secure routing', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.192–201.

Bonato, P. (2003, May/June) 'Wearable sensors/systems and their impact on biomedical engineering', *IEEE Engineering in Medicine and Biology Magazine*, Vol. 22, No. 2, pp.18–20.

Bonato, P., Mork, P., Sherrill, D. and Weggaard, R. (2003 May/June) 'Data mining of motor patterns recorded with wearable technology', *IEEE Engineering in Medicine and Biology Magazine*, Vol. 22, No. 3, pp.110–119.

Bouhoula, A., Trabelsi, Z., Barka, E. and Benelbahri, M. (2008) 'Firewall filtering rules analysis for anomalies detection', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.161–172.

Brown, L. (1996) *Modern Private Key Ciphers (part 1)*. Available online at: http://williamstallings.com/Extras/Security-Notes/lectures/blockA.html (accessed on 13 October 2010).

Buchanan, B.G. and Shortliffe, H. (1984) *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison-Wesley, Reading, MA.

Buhan, I., Boom, B., Doumen, J., Hartel, P.H. and Veldhuis, R.N.J. (2009) 'Secure pairing with biometrics', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.27–42.

Burt, A.L., Darschewski, M., Ray, I., Thurimella, R. and Wu, H. (2008) 'Origins: an approach to trace fast spreading worms to their roots', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.36–46.

Bussmann, J., Tulen, J., van Herel, E. and Stam, H. (1998) 'Quantification of physical activities by means of ambulatory accelerometry: a validation study', *Psychophysiology*, Vol. 35, No. 5, pp.488–496.

Chakrabarti, S., Chandrasekhar, S. and Singhal, M. (2009) 'An escrow-less identity-based group-key agreement protocol for dynamic peer groups', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.171–188.

Challal, Y., Gharout, S., Bouabdallah, A. and Bettahar, H. (2008) 'Adaptive clustering for scalable key management in dynamic group communications', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.133–146.

Chen, B., Muniswamy-Reddy, K. and Welsh, M. (2006) 'Ad-hoc multicast routing on resource-limited sensor nodes', *Proceedings of 2nd ACM/Sigmobile Workshop on Multi-hop Ad Hoc Networks: From Theory to Reality (REALMAN'06)*, 26 May, Florence, Italy, pp.87–94.

Chen, H. and Guizani, M. (2007) 'Editorial', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.1–2.

Chen, Z., Chen, C. and Li, Y. (2009) 'Deriving a closed-form expression for worm-scanning strategies', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.135–144.

Chen, Z., Chen, C. and Wang, Q. (2010) 'On the scalability of Delay-Tolerant Botnets', *International Journal of Security and Networks*, Vol. 5, No. 4, pp.248–258.

Chen, Z. and Ji, C. (2007) 'Optimal worm-scanning method using vulnerable-host distributions', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.71–80.

Cheng, Z. and Chen, L. (2007) 'On security proof of McCullagh–Barreto's key agreement protocol and its variants', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.251–259.

Cherukuri, S., Venkatasubramanian, K.K. and Gupta, S.K.S. (2003) 'BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body', *IEEE Proceedings of International Conference on Parallel Processing Workshops*, 6–9 October, pp.432–439.

Chiti, F., Fantacci, R., Archetti, F., Messina, E. and Toscani, D. (2009) 'An integrated communications framework for context aware continuous monitoring with body sensor networks', *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless and Pervasive Communications for Healthcare*, Vol. 27, No. 4, pp.379–386.

Chobanian, A.V., Bakris, G.L., Black, H.R., Cushman, W.C., Green, L.A., Izzo Jr, J.L., Jones, D.W., Materson, B.J., Oparil, S., Wright Jr., J.T., Roccella, E.J. and National High Blood Pressure Education Program Coordinating Committee (2003) 'The seventh report of the joint national committee on prevention, detection, evaluation, and treatment of high blood pressure', *Hypertension*, Vol. 42, No. 6, pp.1206–1252.

Cronin, E., Sherr, M. and Blaze, M. (2008) 'On the (un)reliability of eavesdropping', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.103–113.

Dalton II, G., Edge, K.S., Mills, R.F. and Raines, R.A. (2010) 'Analysing security risks in computer and radio frequency identification (RFID) networks using attack and protection trees', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.87–95.

De Couto, D.S.J., Aguayo, D., Bicket, J. and Morris, R. (2003) 'A high-throughput path metric for multi-hop wireless routing', *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, 14–19 September, San Diego, CA, USA, pp.134–146.

DICOM (2010) *DICOM Strategic Document, Version 10.0*. Available online at: http://medical.nema.org/dicom/geninfo/Strategy.pdf (accessed on 13 October 2010).

Dishman, E. (2004) 'Inventing wellness systems for aging in place', *IEEE Computer*, Vol. 37, No. 5, pp.34–41.

Djenouri, D., Bouamama, M. and Mahmoudi, O. (2009) 'Black-hole-resistant ENADAIR-based routing protocol for mobile ad hoc networks', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.246–262.

Dong, Y., Hsu, S., Rajput, S. and Wu, B. (2010) 'Experimental analysis of application-level intrusion detection algorithms', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.198–205.

Drakakis, K.E., Panagopoulos, A.D. and Cottis, P.G. (2009) 'Overview of satellite communication networks security: introduction of EAP', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.164–170.

Drugge, M., Hallberg, J., Parnes, P. and Synnes, K. (2006) 'Wearable systems in nursing home care: prototyping experience', *IEEE Pervasive Computing*, Vol. 5, No. 1, pp.87–91.

Durbin, D. (2000) *Rapid Interpretation of EKGs*, 6th ed., Cover Publishing Company, Tampa, FL.

Dutta-Roy, A. (1999) 'Networks for homes', *IEEE Spectrum*, Vol. 36, No. 12, pp.26–33.

Ehlert, S., Rebahi, Y. and Magedanz, T. (2009) 'Intrusion detection system for denial-of-service flooding attacks in SIP communication networks', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.189–200.

Erdogan, O. and Cao, P. (2007) 'Hash-AV: fast virus signature scanning by cache-resident filters', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.50–59.

Finnigin, K.M., Mullins, B.E., Raines, R.A. and Potoczny, H.B. (2007) 'Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.260–271.

Furse, C., Lai, H.K., Estes, C., Mahadik, A. and Duncan, A. (1999) 'An implantable antenna for communication with implantable medical devices', *Proceedings of IEEE Antennas and Propagation/URSI International Symposium*, Orlando, FL, USA.

Furse, C., Mohan, R., Jakayar, A., Karidehal, S., McCleod, B. and Going, S. (2002) 'A biocompatible antenna for communication with implantable medical devices', *Proceedings of the IEEE International Symposium on Antennas and Propagation*, San Antonio, TX, USA.

Gao, T., Greenspan, D., Welsh, M., Juang, R.R. and Alm, A. (2005, September) 'Vital signs monitoring and patient tracking over a wireless network', *Proceedings of the 27th Annual International Conference of the IEEE EMBS*, Shanghai, China, pp.102–105.

Gaynor, M., Messer, R., Myung, D. and Moulton, S. (2006, May) 'Application for emergency medical services', *Proceedings of the 3rd International ISCRAM Conference*, Newark, NJ, USA.

Gaynor, M., Myung, D., Patel, R. and Moulton, S. (2007) 'Human computer interaction in the pre-hospital setting', *Proceedings of the 40th Annual Hawaii international Conference on System Sciences*, 3–6 January, Big Island, HI, USA.

Gemperle, F., Kasabach, C., Stivoric, J., Bauer, M. and Martin, R. (1998) 'Design for wearability', *Proceedings of the 2nd IEEE International Symposium on Wearable Computers*, 19–20 October 1998, Pittsburgh, PA, USA, pp.116–122.

Goodrich, M., Sirivianos, M., Solis, J., Soriente, C., Tsudik, G. and Uzun, E. (2009) 'Using audio in secure device pairing', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.57–68.

Gu, Q., Liu, P., Chu, C. and Zhu, S. (2007) 'Defence against packet injection in ad hoc networks', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.154–169.

Guo, H., Mu, Y., Zhang, X.Y. and Li, Z.J. (2010) 'Enhanced McCullagh-Barreto identity-based key exchange protocols with master key forward security', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.173–187.

Guo, Y. and Perreau, S. (2010) 'Detect DDoS flooding attacks in mobile ad hoc networks', *International Journal of Security and Networks*, Vol. 5, No. 4, pp.259–269.

Hackney, D.H. (2005) *Wireless Telemedicine for Nursing Homes and Retirement Centers*, Bachelor of Commuter Science Thesis, University of Virginia, USA.

Heinzelman, W.R., Chandrakasan, A. and Balakrishnan, H. (2000) 'Energy-efficient communication protocol for wireless microsensor networks', *Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8*, 4–7 January, IEEE Computer Society, Washington, DC, USA, pp.3005–3014.

Helal, S., Winkler, B., Lee, C., Kaddoura, Y., Ran, L., Giraldo, C., Kuchibhotla, S. and Mann, W. (2003) 'Enabling location-aware pervasive computing applications for the elderly', *Proceedings of 1st IEEE International Conference on Pervasive Computing and Communication*, 23–26 March, PERCOM, IEEE Computer Society, Washington, DC, pp.531–536.

Hoeper, K. and Gong, G. (2007) 'Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.239–250.

Hsiao, Y. and Hwang, R. (2010) 'An efficient secure data dissemination scheme for grid structure wireless sensor networks', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.26–34.

Hsieh, C., Chen, J., Lin, Y-B., Chen, K., Liao, H. and Liang, C. (2008) 'NTP-DownloadT: a conformance test tool for secured mobile download services', *International Journal of Security and Networks*, Vol. 3, No. 4, pp.240–249.

Hsu, H., Zhu, S. and Hurson, A.R. (2007) 'LIP: a lightweight interlayer protocol for preventing packet injection attacks in mobile ad hoc network', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.202–215.

Hu, F. and Kumar, S. (2003) 'QoS considerations in wireless sensor networks for telemedicine', *Proceedings of SPIE ITCOM Conference*, Orlando, FL, USA.

Hu, F., Celentano, L. and Xiao, Y. (2009a) 'Error-resistant RFID-assisted wireless sensor networks for cardiac telehealthcare', *Wireless Communications and Mobile Computing (WCMC) Journal*, Vol. 9, No. 1, pp.85–101.

Hu, F., Dong, D. and Xiao, Y. (2009b) 'Attacks and countermeasures in multi-hop cognitive radio networks', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.263–271.

Hu, F., Jiang, M. and Xiao, Y. (2008a) 'Low-cost wireless sensor networks for remote cardiac patients monitoring applications', *Wireless Communications and Mobile Computing*, Vol. 8, No. 4, pp.513–529.

Hu, F., Jiang, M., Celentano, L. and Xiao, Y. (2008b) 'Robust medical ad hoc sensor networks (MASN) with wavelet-based ECG data mining', *Ad Hoc Network*, Vol. 6, No. 7, pp.986–1012.

Hu, F., Kumar, S. and Xiao, Y. (2006a) 'Towards a secure, RFID/Sensor based tele-cardiology system', *IEEE CCNC'07*, 5 September, pp.732–736.

Hu, F., Rughoonundon, A. and Celentano, L. (2008c) 'Towards a realistic testbed for wireless network reliability and security performance studies', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.63–77.

Hu, F., Wang, Y. and Wu, H. (2006b) 'Mobile telemedicine sensor networks with low-energy data query and network lifetime considerations', *IEEE Transactions on Mobile Computing*, Vol. 5, No. 4, pp.404–417.

Hu, F., Xiao, Y. and Hao, Q. (2009c) 'Congestion-aware, loss-resilient bio-monitoring sensor networking for mobile health applications', *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless and Pervasive Communications for Healthcare*, Vol. 27, No. 4, pp.450–465.

Huang, D. (2007) 'Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.272–283.

Huang, H., Kirchner, H., Liu, S. and Wu, W. (2009) 'Handling inheritance violation for secure interoperation of heterogeneous systems', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.223–233.

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

Hung, K. and Zhang, Y.T. (2003) 'Implementation of a WAP-based telemedicine system for patient monitoring', *IEEE Transactions on Information Technology in Biomedicine*, Vol. 7, No. 2, pp.101–107.

Hutter, M., Plos, T. and Feldhofer, M. (2010) 'On the security of RFID devices against implementation attacks', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.106–118.

IEEE 802.11-1999 Part 11 (1999, August) *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, Standard IEEE.

Imasaki, Y., Zhang, Y. and Ji, Y. (2010) 'Secure and efficient data transmission in RFID sensor networks', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.119–127.

Intel (2004) *Intel Showcases Innovative Wireless Sensor Networks for In-Home Health Care Solutions*. Available online at: http://www.intel.com/pressroom/archive/releases/20040316corp.htm (accessed on 13 October 2010).

Istepanian, R.S.H., Jovanov, E. and Zhang, Y.T. (2004) 'Guest editorial introduction to the special section on M-health: beyond seamless mobility and global wireless health-care connectivity', *IEEE Transactions on Information Technology in Biomedicine*, Vol. 8, No. 4, pp.405–414.

Jain, A., Ross, A. and Prabhakar, S. (2004) 'An introduction to biometric recognition', *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp.4–20.

Jara, A.J., Zamora-Izquierdo, M.A. and Gomez-Skarmeta, A.F. (2009) 'An ambient assisted living system for telemedicine with detection of symptoms', *Bioinspired Applications in Artificial and Natural Computation*, Lecture Note in Computer Science, Springer, Vol. 5602, pp.75–84.

Jovanov, E., Milenkovic, A., Otto, C. and de Goroen, P.C. (2005) 'A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation', *Journal of NeuroEngineering and Rehabilitation*, Vol. 2, No. 6.

Kalogridis, G., Denic, S.Z., Lewis, T. and Cepeda, R. (2011) 'Privacy protection system and metrics for hiding electrical events', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.14–27.

Kandikattu, R. and Jacob, L. (2008) 'Secure hybrid routing with micro/macro-mobility handoff mechanisms for urban wireless mesh networks', *International Journal of Security and Networks*, Vol. 3, No. 4, pp.258–274.

Kilpatrick, T., Gonzalez, J., Chandia, R., Papa, M. and Shenoi, S. (2008) 'Forensic analysis of SCADA systems and networks', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.95–102.

Korkmaz, T., Gong, C., Sarac, K. and Dykes, S. (2007) 'Single packet IP traceback in AS-level partial deployment scenario', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.95–108.

Kotzanikolaou, P., Vergados, D.D., Stergiou, G. and Magkos, E. (2008) 'Multilayer key establishment for large-scale sensor networks', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.1–9.

Krupinski, E.A., Webster, P., Dolliver, M., Weinstein, R.S. and Lopez, A.M. (1999) 'Efficiency analysis of a multi-specialty telemedicine service', *Telemedicine Journal*, Vol. 5, No. 3, pp.265–271.

Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T. and Butler-Purry, K.L. (2011) 'Towards modelling the impact of cyber attacks on a smart grid', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.2–13.

Kuo, C., Perrig, A. and Walker, J. (2009) 'Designing user studies for security applications: a case study with wireless network configuration', *International Journal of Security and Networks*, Vol. 409, Nos. 1/2, pp.101–109.

Kyriacou, E., Pavlopoulos, S., Bourka, A., Berler, A. and Koutsouris, D. (1999, September) 'Telemedicine in emergency care', *Proceedings of the VI International Conference on Medical Physics*, Patra, Greece, pp.293–298.

Kyriacou, E., Pavlopoulos, S., Koutsouris, D., Andreou, A., Pattichis, C. and Schizas, C. (2001) 'Multipurpose health care telemedicine system', *Proceedings of the 23rd Annual International Conference of the IEEE/EMBS*, Istanbul, Turkey, pp.3544–3547.

Lau, M. (1998) *GeoPak: Monitoring Climbers and Climate on Mount Everest*, Masters of Engineering Thesis, MIT, Cambridge, MA, USA.

Laur, S. and Pasini, S. (2009) 'User-aided data authentication', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.69–86.

Lee, S. and Sivalingam, K.M. (2009) 'An efficient one-time password authentication scheme using a smart card', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.145–152.

Leng, X., Lien, Y., Mayes, K. and Markantonakis, K. (2010) 'An RFID grouping proof protocol exploiting anti-collision algorithm for subgroup dividing', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.79–86.

Li, F., Luo, B. and Liu, P. (2011) 'Secure and privacy-preserving information aggregation for smart grids', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.28–39.

Li, F., Srinivasan, A. and Wu, J. (2008a) 'PVFS: a probabilistic voting-based filtering scheme in wireless sensor networks', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.173–182.

Li, F., Xin, X. and Hu, Y. (2008b) 'ID-based threshold proxy signcryption scheme from bilinear pairings', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.206–215.

Li, R., Li, J. and Chen, H. (2007) 'DKMS: distributed hierarchical access control for multimedia networks', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.3–10.

Lin, X., Ling, X., Zhu, H., Ho, P. and Shen, X. (2008) 'A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.122–132.

Ling, H. and Znati, T. (2007) 'End-to-end pairwise key establishment using node disjoint secure paths in wireless sensor networks', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.109–121.

Liszka, K.J. (2007, January) 'A sensor network architecture for cardiac health monitoring', *The 4th IEEE Consumer Communications and Networking Conference (CCNC 2007)*, Las Vegas, NV, USA, pp.737–740.

Liszka, K.J., Macking, M.A., Lichter, M.J., York, D.W., Pillai, D. and Resenbaum, D.S. (2004a) 'Keeping a beat on the heart', *IEEE Pervasive Computing*, Vol. 3, No. 4, pp.42–49.

Liszka, K.J., York, D.W., Mackin, M.A. and Lichter, M.J. (2004b, June) 'Remote monitoring of a heterogeneous sensor network for biomedical research in space', *Proceedings of the International Conference on Pervasive Computing and Communications*, CSREA Press, pp.829–833.

Ma, L., Teymorian, A.Y., Xing, K. and Du, D. (2008) 'An one-way function based framework for pairwise key establishment in sensor networks', *International Journal of Security and Networks*, Vol. 3, No. 4, pp.217–225.

Ma, X. and Cheng, X. (2008) 'Verifying security protocols by knowledge analysis', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.183–192.

Mahinderjit-Singh, M. and Li, X. (2010) 'Trust in RFID-enabled supply-chain management', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.96–105.

Malan, D., Fulford-Jones, T., Welsh, M. and Moulton, S. (2004, April) 'CodeBlue: an ad hoc sensor network infrastructure for emergency medical care', *International Workshop on Wearable and Implantable Body Sensor Networks*, London, UK.

Malaney, R. (2007) 'Securing Wi-Fi networks with position verification: extended version', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.27–36.

Malliga, S. and Tamilarasi, A. (2010) 'A backpressure technique for filtering spoofed traffic at upstream routers', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.3–14.

Malmivuo, J. and Plonsey, R. (1995) *Bioelectromagnetism*, Oxford University Press, New York.

Mathie, M., Coster, A., Lovell, N. and Celler, B. (2004, April) 'Accelerometry: providing an integrated, practical method for long-term, ambulatory monitoring of human movement', Physiological Measurement, Vol. 25, No. 2.

Mayrhofer, R., Nyberg, K. and Kindberg, T. (2009) 'Foreword', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.1–3.

McCune, J., Perrig, A. and Reiter, M. (2009) 'Seeing-is-believing: using camera phones for human-verifiable authentication', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.43–56.

Memon, N. and Goel, R. (2008) 'Editorial', *International Journal of Security and Networks*, Vol. 3, No. 2, p.79.

Menezes, A., van Oorschot, P. and Vanstone, S. (1997) *Handbook of Applied Cryptography*, CRC Press.

Michail, H.E., Panagiotakopoulos, G.A., Thanasoulis, V.N., Kakarountas, A.P. and Goutis, C.E. (2007) 'Server side hashing core exceeding 3 Gbps of throughput', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.228–238.

Milenković, A., Otto, C. and Jovanov, E. (2006) 'Wireless sensor networks for personal health monitoring: issues and an implementation', *Computer Communications*, Vol. 29, Nos. 13/14, pp.2521–2533.

Mišić, J., Amini, F. and Khan, M. (2007, January.) 'On security attacks in healthcare WSNs implemented on 802.15.4 beacon enabled clusters', *The 4th IEEE Conference on Consumer Communications and Networking (CCNC 2007)*, Las Vegas, NV, USA, pp.741–745.

Mišić, J. and Mišić, V.B. (2007) 'Implementation of security policy for clinical information systems over wireless sensor networks', *Ad Hoc Networks*, Vol. 5, No. 1, pp.134–144.

Mu, Y., Chen, L., Chen, X., Gong, G., Lee, P., Miyaji, A., Pieprzyk, J., Pointcheval, D., Takagi, T., Traore, J., Seberry, J., Susilo, W., Wang, H. and Zhang, F. (2007) 'Editorial', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.171–174.

Negus, K.J., Stephens, A.P. and Lansford, J. (2000) 'Home RF: wireless networking for the connected home', *IEEE Personal Communications*, Vol. 7, No. 1, pp.20–27.

Okolica, J.S., Peterson, G.L. and Mills, R.F. (2008) 'Using PLSI-U to detect insider threats by datamining e-mail', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.114–121.

Oliveira, L.B., Wong, H., Loureiro, A.A.F. and Dahab, R. (2007) 'On the design of secure protocols for hierarchical sensor networks', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.216–227.

Olteanu, A. and Xiao, Y. (2010) 'Security overhead and performance for aggregation with fragment retransmission (AFR) in very high-speed wireless 802.11 LANs', *IEEE Transactions on Wireless Communications*, Vol. 9, No. 1, pp.218–226.

Palatini, P. (1999) 'Need for a revision of the normal limits of resting heart rate', *Hypertension*, Vol. 33, No. 2, pp.622–625.

Pan, J., Cai, L. and Shen, X. (2007) 'Vulnerabilities in distance-indexed IP traceback schemes', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.81–94.

Pan, J. and Tompkins, W.J. (1985) 'A real-time QRS detection algorithm', *IEEE Transactions on Biomedical Engineering*, Vol. 32, No. 3, pp.230–236.

Pattichis, C.S., Kyriacou, E., Voskarides, S., Pattichis, M.S., Istepanian, R. and Shizas, C.N. (2002) 'Wireless telemedicine systems: an overview', *IEEE Antennas & Propagation Magazine*, Vol. 44, No. 2, pp.143–153.

Pavlopoulos, S., Kyriacou, E., Berler, A., Dembeyiotis, S. and Koutsouris, D. (1998) 'A novel emergency telemedicine system based on wireless communication technology – AMBULANCE', *IEEE Transactions On Informatics Technology Biomedicine*, Vol. 2, No. 4, pp.261–267.

Ponyik, J.G. and York, D.W. (2002, March) 'Embedded web technology: applying world wide web standards to embedded systems', *NASA TM-2002-211199*, AIAA-2001-5107.

Poon, C.C.Y. and Zhang, Y. (2005, September) 'Cuff-less and noninvasive measurements of arterial blood pressure by pulse transit time', *Proceedings of 27th IEEE International Conference of Engineering in Medicine and Biology Society*, Shanghai, China, pp.5877–5880.

Poon, C.C.Y., Zhang, Y. and Bao, S. (2006) 'A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-Health', *IEEE Communications Magazine*, Vol. 44, No. 4, pp.73–81.

Prakash, Y., Lalwani, S., Gupta, S.K.S., Elsharawy, E. and Schwiebert, L. (2003) 'Towards a propagation model for wireless biomedical applications', *IEEE ICC 2003*, Vol. 3, pp.1993–1997.

Proakis, J.G. and Salehi, M. (1994) *Communication Systems Engineering*, Prentice Hall, New Jersey, USA.

Raad, M. (2010) 'A ubiquitous mobile telemedicine system for the elderly using RFID', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.156–164.

Rabinovich, P. and Simon, R. (2007) 'Secure message delivery in publish/subscribe networks using overlay multicast', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.60–70.

Ramsey, B.W., Mullins, B.E., Thomas, R.W. and Andel, T.R. (2011) 'Subjective audio quality over a secure IEEE 802.11n network', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.53–63.

Rao, S.P., Jayant, N.S., Stachura, M.E., Astapova, E. and Pearson-Shaver, A. (2009) 'Delivering diagnostic quality video over mobile wireless network for telemedicine', *International Journal of Telemedicine and Applications*, Vol. 2009, pp.1–9.

Ray, I. and Poolsappasit, N. (2008) 'Using mobile ad hoc networks to acquire digital evidence from remote autonomous agents', *International Journal of Security and Networks*, Vol. 3, No. 2, pp.80–94.

Rekhis, S. and Boudriga, N.A. (2009) 'Visibility: a novel concept for characterising provable network digital evidences', *International Journal of Security and Networks*, Vol. 4, No. 4, pp.234–245.

Richard, A.O., Ahmad, A. and Kiseon, K. (2010) 'Security assessments of IEEE 802.15.4 standard based on X.805 framework', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.188–197.

Rodrigues, M.J. and James, K. (2010) 'Perceived barriers to the widespread commercial use of radio frequency identification technology', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.165–172.

Rosenbaum, D.S., Albrecht, P. and Cohen, R.J. (1996) 'Predicting sudden cardiac death from microvolt T-wave alternans of the surface electrocardiogram: promise and pitfalls', *Journal of Cardiovascular Electrophysiology*, Vol. 7, pp.1095–1111.

Rosenbaum, D.S., Jackson, L.E., Smith, J.M., Garan, H., Ruskin, J.N. and Cohen, R.J. (1994) 'Electrical alternans and vulnerability to ventricular arrhythmias', *New England Journal of Medicine*, Vol. 330, pp.235–241.

Rowstron, A. and Druschel P. (2001) 'Pastry: scalable, distributed object location and routing for large-scale peer-to-peer systems', *Proceedings of 4th IFIP/ACM International Conferences on Distributed Systems Platforms*, ACM Press, pp.329–350.

Sadowitz, M., Latifi, S. and Walker, D. (2008) 'An iris and retina multimodal biometric system', *International Journal of Security and Networks*, Vol. 3, No. 4, pp.250–257.

Sakarindr, P. and Ansari, N. (2007) 'Adaptive trust-based anonymous network', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.11–26.

Scannell, A., Varshavsky, A., LaMarca, A. and Lara, E.D. (2009) 'Proximity-based authentication of mobile devices', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.4–16.

Scheirer, W. and Chuah, M. (2008) 'Syntax vs. semantics: competing approaches to dynamic network intrusion detection', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.24–35.

Schrader, K.R., Mullins, B.E., Peterson, G.L. and Mills, R.F. (2010) 'An FPGA-based system for tracking digital information transmitted via peer-to-peer protocols', *International Journal of Security and Networks*, Vol. 5, No. 4, pp.236–247.

Schwartz, G.R. (1999) *Principles and Practice of Emergency Medicine*, Rittenhouse Book Distributors, King of Prussia, PA.

Schwiebert, L., Gupta, S.K.S., Auner, P.S.G., Abrams, G., Lezzi, R. and McAllister, P. (2002) 'A biomedical smart sensor for the visually impaired', *1st IEEE International Conference on Sensors*, 11–14 June, Orlando, FL, USA.

Schwiebert, L., Gupta, S.K.S. and Weinmann, J. (2001) 'Research challenges in wireless networks of biomedical sensors', *Proceedings of the 7th Annual international Conference on Mobile Computing and Networking*, Rome, Italy, pp.151–165.

Shankar, V., Natarajan, A., Gupta, S.K.S. and Schwiebert, L. (2001, September) 'Energy-efficient protocols for wireless communication in biosensor networks', *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 1, pp.114–118.

Shnayder, V., Chen, B., Lorincz, K., Jones, T.R. and Welsh, M. (2005) 'Sensor networks for medical care', *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, 2–4 November, San Diego, USA.

Soriente, C., Tsudik, G. and Uzun, E. (2009) 'Secure pairing of interface constrained devices', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.17–26.

Srinivasan, A., Li, F., Wu, J. and Li, M. (2008) 'Clique-based group key assignment in wireless sensor networks', *International Journal of Security and Networks*, Vol. 3, No. 4, pp.226–239.

Studer, M.A. (1999) *The Evolution of Telemedicine in Celestial and Terrestrial Realms*. Available online at: http://www.space.edu/public/publications/abstracts/jensen/studer.html (accessed on 1 October 2003).

Sufi, F., Fang, Q., Khalil, I. and Mahmoud, S.S. (2009) 'Novel methods of faster cardiovascular diagnosis in wireless telecardiology', *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless and Pervasive Communications for Healthcare*, Vol. 27, No. 4, pp.537–552.

Sun, F. and Shayman, M. (2007) 'On pairwise connectivity of wireless multihop networks', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.37–49.

Sun, L. (2010) 'Security and privacy on low-cost radio frequency identification systems', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.128–134.

Suomalainen, J., Valkonen, J. and Asokan, N. (2009) 'Standards for security associations in personal networks: a comparative analysis', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.87–100.

Takahashi, D., Xiao, Y., Hu, F., Chen, J. and Sun, Y. (2008) 'Temperature aware routing for telemedicine applications in embedded biomedical sensor networks', *EURASIP Journal on Wireless Communications and Networking, Special Issue on "Wireless Telemedicine and Applications",* Vol. 2008, No. 2, 11p.

Taleb, T., Bottazzi, D., Guizani, M. and Nait-Charif, H. (2009) 'ANGELAH: a framework for assisting elders at home', *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless and Pervasive Communications for Healthcare*, Vol. 27, No. 4, pp.480–494.

Tang, Q., Tummala, N., Gupta, S.K.S. and Schwiebert, L. (2005) 'TARA: thermal-aware routing algorithm for implanted sensor networks', *Proceedings of the International Conference on Distributed Computing in Sensor Systems*, pp.206–217.

Tartary, C. and Wang, H. (2007) 'Efficient multicast stream authentication for the fully adversarial network model', *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp.175–191.

Te'eni, D., Carey, J. and Zhang, P. (2007) *Human Computer Interaction: Developing Effective Organizational Information Systems*, Wiley, Hoboken, NJ.

Tripathy, S. and Nandi, S. (2008) 'Secure user-identification and key distribution scheme preserving anonymity', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.201–205.

Tsai, K., Hsu, C. and Wu, T. (2010) 'Mutual anonymity protocol with integrity protection for mobile peer-to-peer networks', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.45–52.

Turner, R.T. (2000, August) 'Physiology of a microgravity environment: invited review: what do we know about the effects of spaceflight on bone?', *Journal of Applied Physiology*, Vol. 89, pp.840-847.

United Nations Population Division (2001) *World Population Prospects: The 2000 Revision*. Available online at: http://www.un.org/spanish/esa/population/wpp2000h.pdf (accessed on 13 October 2010).

Uphoff, B. and Wong, J.S. (2008) 'An agent-based framework for intrusion detection alert verification and event correlation', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.193–200.

US HHS (2002) *Standards for Privacy of Individually Identifiable Health Information (Final Rule)*. Available online at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (accessed on 13 October 2010).

Wang, H. and Jia, X. (2010) 'Editorial', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.77–78.

Wang, J. and Smith, G.L. (2010) 'A cross-layer authentication design for secure video transportation in wireless sensor network', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.63–76.

Wang, W., Kong, J., Bhargava, B. and Gerla, M. (2008) 'Visualisation of wormholes in underwater sensor networks: a distributed approach', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.10–23.

Wang, Z. and Gu, H. (2009) 'A review of telemedicine in China', *Journal of Telemedicine and Telecare*, Vol. 15, pp.23–27.

Watkins, L., Beyah, R. and Corbett, C. (2009) 'Using link RTT to passively detect unapproved wireless nodes', *International Journal of Security and Networks*, Vol. 4, No. 3, pp.153–163.

Webopedia (2010) *Mote*. Available online at: http://www.webopedia.com/TERM/M/mote.html (accessed on 13 October 2010).

Welsh, M. (2005) *CodeBlue: A Wireless Sensor Network for Medical Care and Disaster Response*. Available online at: http://www.eecs.harvard.edu/~mdw/talks/ucsd-codeblue.pdf (accessed on 13 October 2010).

Welsh, M., Malan, D., Duncan, B., Fulford-Jones, T. and Moulton, S. (2004) *Wireless Sensor Networks for Emergency Medical Care*. Available online at: http://www.cs.usask.ca/faculty/ludwig/SensorGrid/docs/E-HEALTH%20PAPERS/codeblue%20SLIDES.pdf (accessed on 13 October 2010).

Welsh, M., Myung, D., Gaynor, M. and Moulton, S. (2003) 'Resuscitation monitoring with a wireless sensor network', *Supplement to Circulation: Journal of the American Heart Association*, 28 October.

Woo, A., Tong, T. and Culler, D. (2003) 'Taming the underlying challenges of reliable multihop routing in sensor networks', *Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys 2003)*, 5–7 November, Los Angeles, CA, USA, pp.14–27.

Wu, B., Wu, J. and Dong, Y. (2009) 'An efficient group key management scheme for mobile ad hoc networks', *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp.125–134.

Xiao, Y. (2011) 'Editorial', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.1–1.

Xiao, Y., Bandela, C., Du, X., Pan, Y. and Dass, K. (2006a) 'Security mechanisms, attacks, and security enhancements for the IEEE 802.11 WLANs', *International Journal of Wireless and Mobile Computing*, Vol. 1, Nos. 3/4, pp.276–288.

Xiao, Y., Dass, K., Zheng, J. and Wu, K. (2007a) 'Temporal key integrity protocol and its security issues in IEEE 802.11i', in Wu, S-L. and Tseng, Y-C. (Eds): *Wireless Ad Hoc Networking: Personal-Area, Local-Area, and Sensory-Area Networks*, Chapter 16, Auerbach Publications, Taylor & Francis Group, New York, pp.419–435.

Xiao, Y. and Li, H. (2004) 'Voice and video transmissions with global data parameter control for the IEEE 802.11e enhance distributed channel access', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 15, No. 11, pp.1041–1053.

Xiao, Y., Shen, X., Sun, B. and Cai, L. (2006b) 'Security and privacy in RFID and applications in telemedicine', *IEEE Communications Magazine, Special Issue on Quality Assurance and Devices in Telemedicine*, pp.64–72.

Xiao, Y., Yu, S., Wu, K., Ni, Q., Janecek, C. and Nordstad, J. (2007b) 'Radio frequency identification: technologies, applications, and research issues', *Journal of Wireless Communications and Mobile Computing*, Vol. 7, No. 4, pp.457–472.

Xu, H., Ayachit, M. and Reddyreddy, A. (2008) 'Formal modelling and analysis of XML firewall for service-oriented systems', *International Journal of Security and Networks*, Vol. 3, No. 3, pp.147–160.

Xu, L., Chen, S., Huang, X. and Mu, Y. (2010) 'Bloom filter based secure and anonymous DSR protocol in wireless ad hoc networks', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.35–44.

Yang, M. (2010) 'Lightweight authentication protocol for mobile RFID networks', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.53–62.

Yang, M., Liu, J.C.L. and Tseng, Y. (2010) 'Editorial', *International Journal of Security and Networks*, Vol. 5, No. 1, pp.1–3.

Zhang, J. and Gunter, C.A. (2011) 'Application-aware secure multicast for power grid communications', *International Journal of Security and Networks*, Vol. 6, No. 1, pp.40–52.

Zhang, X., Gao, Q. and Saad, M.K. (2010) 'Looking at a class of RFID APs through GNY logic', *International Journal of Security and Networks*, Vol. 5, Nos. 2/3, pp.135–146.

Zhu, Y., Fu, X., Bettati, R. and Zhao, W. (2007) 'Analysis of flow-correlation attacks in anonymity network', *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp.137–153.

Zhuang, Z., Li, Y. and Chen, Z. (2010) 'Enhancing intrusion detection system with proximity information', *International Journal of Security and Networks*, Vol. 5, No. 4 pp.207–219.

Zou, X. and Karandikar, Y. (2008) 'A novel conference key management solution for secure dynamic conferencing', *International Journal of Security and Networks*, Vol. 3, No. 1, pp.47–53.