Mobile Information Systems 2 (2006) 151–167
IOS Press

Bluetooth: Opening a blue sky for healthcare

X.H. Wang* and M. Iqbal
Faculty of Computing, Information Systems and Mathematics, Kingston University, Kingston upon Thames, KT1 2EE, UK

Abstract. Over the last few years, there has been a blossoming of developing mobile healthcare programs. Bluetooth technology, which has the advantages of being low-power and inexpensive, whilst being able to transfer moderate amounts of data over a versatile, robust and secure radio link, has been widely applied in mobile healthcare as a replacement for cables. This paper discussed the applications of Bluetooth technology in healthcare. It started with the brief description of the history of Bluetooth technology, its technical characteristics, and the latest developments. Then the applications of Bluetooth technology in healthcare sector were reviewed. The applications are based on two basic types of links of Bluetooth technology: point-to-point link and point-to-multipoint link. The special requirements from healthcare and the challenges of successful application of Bluetooth in healthcare will be discussed. At last the future development of Bluetooth technology and its impacts on healthcare were envisioned.

Keywords: Mobile healthcare, bluetooth, patient monitoring

1. Introduction

The application of wireless technology in healthcare is not new. The notation of using radios in healthcare dates back to the 1920s. During that time, radios were used to link physicians at shore stations to assist ships at sea that had medical emergencies. Perhaps the first proof is the article "The Radio Doctor – Maybe!" appeared in "Radio News" magazine in April 1924 [1]. Since then, each step of the innovation of the wireless technology left footprints on healthcare. For example, the inventions of two-way radio in 1940s, radio pager in 1950s, satellite in 1960s, and mobile phones in 1980s have all the records in healthcare. Among these efforts, the National Aeronautics and Space Administration (NASA) played an important role in the new wave of development of telemedicine projects from early 1960s to support its astronauts in the space [2]. Some of its projects are still valuable nowadays.

Since the mid-1990s, telemedicine programs have become common throughout the world. Owing to the advances of wireless communication, computing and electronics technologies, the application of wireless in healthcare has been evolved into mobile health, which is the synergies of mobile computing, medical sensor, and communications technologies [3]. The objectives of the recent developments of the mobile health programs have been changed from assisting patients in remote area to providing high quality services which are cost-effective and convenient.

Bluetooth technology, designed as cable replacement, has the advantages of being low-power and inexpensive, whilst being able to transfer moderate amounts of data over a versatile, robust and secure

*Corresponding author: Dr. X.H. Wang, Faculty of Computing, Information Systems and Mathematics, Kingston University, Kingston upon Thames, Surrey, KT1 2EE, UK. Tel.: +44 020 85472000 Ext: 62495; Fax: +44 020 8547 7197; E-mail: Xinheng.Wang@kingston.ac.uk.

radio link. It has attracted the attention in healthcare sector from its emergence. Nowadays, Bluetooth has been applied in patient monitoring [4], electronic patient record (EPR) [12], prescription [13] and hearing care [14]. The main area is the remote monitoring of vital signs for patients away from medical environment.

This paper will discuss the applications of Bluetooth technology in healthcare. The history and technical characteristics of the technology and its latest development will be described first. After that two detailed examples are given to investigate how to apply Bluetooth in healthcare. At last the special requirements from healthcare, the challenges of successful application of Bluetooth, and the impacts of future development on healthcare will be discussed.

2. History of bluetooth technology

The Bluetooth technology was discovered by Eriksson in 1994 during a study to find a low-power, low-cost radio interface between mobile phones and their accessories. The solution to this was called Muliticommunication Link at the beginning of 1997. Erickson decided to give the technology away free of charge to any company to use.

Sooner it was realized that in order to keep the uniformity of the technology development there is a need to develop technology specification. In February 1998, five companies Ericsson, Nokia, IBM, Toshiba and Intel formed a Special Interest Group (SIG) to develop standard for the technology. The standard was called "Bluetooth" after the name of Danish king Harald Blatand (known as Harold Bluetooth in English) who united countries of Norway, Sweden, and Denmark, giving the hope of Bluetooth to unite the different industries such as the computing, mobile phone, and automotive markets.

SIG is driving development of the technology and bringing it to market. By December 1, 1999, 3Com, Lucent, Microsoft and Motorola had joined the SIG and all nine members formed a Promoter Group. All other companies can join SIG either at Associate Member level or Adopter Member level. Now it has over 4000 members who are leaders in the telecommunications, computing, automotive, music, apparel, industrial automation, and network industries

3. Bluetooth technology

Bluetooth technology operates at unlicensed ISM (Industrial, Scientific and Medical) 2.4 GHz frequency band. This band is available from 2.4 to 2.4835 GHz in most of the countries around the world and free to use. However this band is currently also being used by Home RF, 802.11 wireless networks, cordless telephones, baby monitors, walkie-talkie, garage door operators, and so on. Bluetooth technology is subject to interference from the above and other resources, such as microwave oven, high-power sodium lights, thunderstorms, overhead cables, and communication channels in other bands, for example, GSM (Global System for Mobile Communications) and CDMA (Code-Division Multiple Access). Bluetooth technology is prone to interference. To achieve a degree of robustness to interference, the Bluetooth system utilizes a frequency-hopping scheme: Frequency Hopping Spread Spectrum (FHSS).

Bluetooth technology is capable of transmitting both data signals (using packet switching) and voice signals (using circuit switching) over a short distance of up to 100 meters. The range of the distance and transmitting power have been specified into three classes. The details of the maximum output power of the transmitter versus range are shown in Table 1.

Unlike GSM and CDMA, who are always on and connected to the network. While a device is connected via Bluetooth, it uses a 3-step procedure to connect to any new device, namely:

Table 1
Bluetooth radio power classes

Power Class	Max Output Power(mW)	Range(m)
Class 1	100	100
Class 2	2.5	10
Class 3	1	1

– Device discovery.
– Service discovery.
– Choose the service.

3.1. Device discovery

Device discovery is the first step to establish link between Bluetooth devices which finds new Bluetooth device in the area. One device serves as a master device allowing other devices to connect to it and the others serve as slave devices.

In the device discovery process, the master device is in *inquiry* and slave device is in *inquiry scan* modes. The master device changes frequencies 3200 times per second. The slave device responds to the inquiry message with changing frequencies once every 1.28 seconds. As the frequency of slave device changes very slowly and the master device changes rapidly, they will ultimately meet on the same frequency. This process will take up to 10.24 seconds.

Once the inquiry is successful, the slave device would enter a *paging scan* mode, where it would wait for a *page* from the master device. The master device would enter the *paging* mode state from the *inquiry* state. In this mode the master device sends the Device Access Code for trying to establish a connection with the slave device. The slave device receives the packet and processes the Device Access Code. Once the packet is received, the slave device returns a response to the master device and then it enters the connection state. The master receives the response and then establishes the connection with the slave device.

3.2. Service discovery

Following device discovery is the service discovery. This process is governed by the Service Discovery Protocol (SDP). It allows a device to retrieve information on services offered by a neighboring device. Once the connection to service discovery is established, requests for information can be transmitted. The SDP also provides functionality for detecting a service is no long available and disconnect after finding the information about any other devices in an area.

3.3. Bluetooth links and states

The Bluetooth devices can be connected via point-to-point connection and point-to-multipoint connection to form a piconet. The slave can also be served as a master allowing other slaves connected to it to form a scatternet. The schematic diagram of the connections is shown in Fig. 1.

The link methods between the point-to-point and point-to-multipoint are different. Synchronous Connection-Oriented (SCO) link is a point-to-point link between a master and a single slave in the piconet. The master maintains the SCO link by using reserved slots at regular intervals. Asynchronous Connection-Less (ACL) link is a point-to-multipoint link between the master and all the slaves participating on the piconet. In the slots not reserved for the SCO link(s), the master can establish an ACL link on a per-slot basis to any slave, including the slave(s) already engaged in an SCO link.

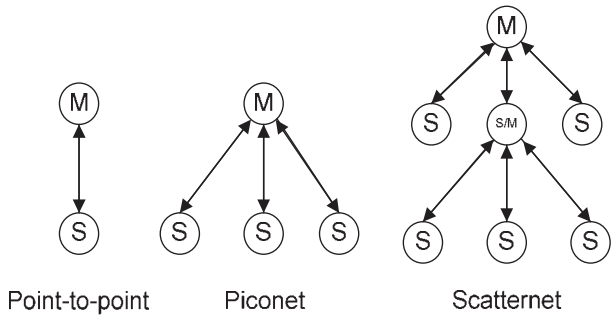

Fig. 1. Schematic diagram of Bluetooth connections.

Following the successful connection, the Bluetooth device can be in any of the four following states: **Active**, **Hold**, **Sniff** and **Park** mode.

In active mode, the Bluetooth device actively participates on the channel. The master schedules the transmission based on traffic demands to and from the different slaves. In addition, it supports regular transmissions to keep slaves synchronized to the channel. Active slaves listen in the master-to-slave slots for packets. If an active slave is not addressed, it may sleep until the next new master transmission.

The next three states are power saving modes. In hold mode, the slave temporarily does not support ACL packets on the channel. The time duration is decided between master and slave prior to the slave entering hold mode. During the hold mode, slave can do other things like scanning, paging, inquiring, or attending another piconet, or entering a low-power sleep mode. When the time is expired, the slave will wake up, synchronize to the traffic on the channel and wait for further master instructions.

Sniff mode: In the sniff mode, the duty cycle of the slave's listen activity can be reduced, thus the master can only transmit in pre-specified time slots. This mode enables the slave to free time in order to accomplish other tasks involving page or inquiry scans.

Park mode: When a slave does not need to participate on the piconet channel, but still wants to remain synchronized to the channel, it can enter the park mode which is a low-power mode with very little activity in the slave. Park mode conserves the most power and would be appropriate for a device in the piconet that would only need to be accessed randomly.

3.4. Bluetooth protocol stacks

As above discussed how the Bluetooth devices work. The communication between Bluetooth devices is defined by the **Bluetooth Protocol Stack,** which is developed by the SIP and is the core of the Bluetooth specification. The main objective of these specifications is to set down the protocols that must be followed by companies when manufacturing and developing both software and hardware to interoperate with each other. To achieve this interoperability, matching applications (e.g., corresponding client and server application) in remote devices must run over identical protocol stacks.

Figure 2 is the architecture of the protocol stack defined by SIP for Version 2 [15]. The stack is divided into two simplest forms: lower stack and upper stack. The lower stack controls all of the physical functionality, the radio, the baseband, and the Link Manger (LM) and Link Controller (LC) layers. The upper stack deals with the channel multiplexing, with the logic link control and adaptation protocol (L2CAP). In addition the Service Discovery Protocol (SDP) is a service layer protocol required by all Bluetooth applications.

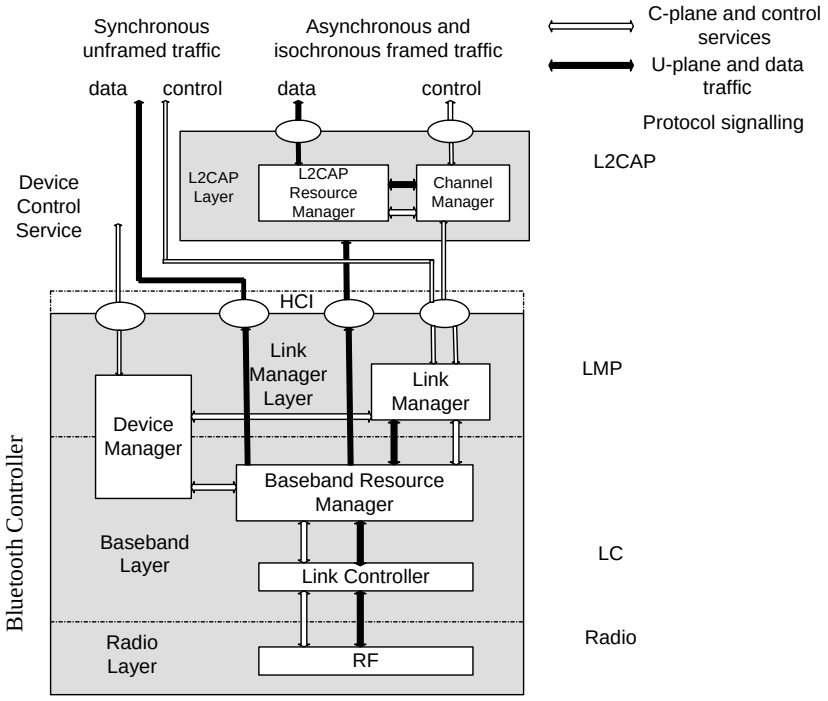

Fig. 2. Bluetooth core system architecture.

Radio Layer The radio layer describes the physical characteristics of the transceiver of a Bluetooth device. These include the modulation and demodulation, radio frequency tolerance, and sensitivity level.

Link Controller layer The link controller is responsible for the encoding and decoding of the Bluetooth packets. It carries out the link control protocol signalling, which is used to communicate flow control and acknowledgement and retransmission request signals.

Baseband resource manager The baseband resource manager is responsible for all access to the radio medium. It has two main functions. One is to grant time on the physical channels to all of the entities that have negotiated an access contract. The other is to negotiate access contracts with these entities. An access contract is effectively a commitment to deliver a certain QoS that is required in order to provide a user application with an expected performance.

Link manager The link manager is responsible for the creation, modification and release of logical links as well as the update of parameters related to physical links between devices. It achieves this by communicating with the link manager in remote Bluetooth devices using the Link Management Protocol (LMP). The LMP uses the links set up by the baseband to establish connections and manage piconets. Responsibilities of the LMP also include authentication and security services, and monitoring of service quality.

It's mentioned above that Bluetooth specification defines two types of links between Bluetooth devices: Synchronous, Connection-Oriented (SCO) link for communications in a piconet and Asynchronous, Connectionless (ACL) link for communication between a single master and slave devices. These two types of links are governed by the link manager.

Device Manger The device manager is the functional block in the baseband that controls the general behaviour of the Bluetooth device. It is responsible for all operation of the Bluetooth system that is not directly related to data transport, such as inquiring for the presence of other nearby Bluetooth devices,

connecting to other Bluetooth devices, or making the local Bluetooth device discoverable or connectable by other devices.

The device manager requests access to the transport medium from the baseband resource controller in order to carry out its functions. The device manager also controls local device behaviour implied by a number of the HCI commands, such as managing the device local name, any stored link keys, and other functionality.

The **HCI** (**host controller interface**) **layer** acts as a boundary between the lower layers of the Bluetooth protocol stack and the upper layers. The Bluetooth specification defines a standard HCI to support Bluetooth systems that are implemented across two separate processors.

L2CAP layer The L2CAP is primarily responsible for:

- Establishing connections across existing ACL links or requesting an ACL link if one does not already exist.
- Multiplexing between different higher layer protocols, such as RFCOMM and SDP, to allow many different applications to use a single ACL link.
- Repackaging the data packets it receives from the higher layers into the form expected by the lower layers.

The L2CAP employs the concept of channels to keep track of where data packets come from and where they should go. You can think of a channel as a logical representation of the data flow between the L2CAP layers in remote devices. Because it plays such a central role in the communication between the upper and lower layers of the Bluetooth protocol stack, the L2CAP layer is a required part of every Bluetooth system.

Above the L2CAP layer, the remaining layers of the Bluetooth protocol stack aren't quite so linearly ordered. However, it makes sense to discuss the service discovery protocol next, because it exists independently of other higher-level protocol layers. In addition, it is common to every Bluetooth device.

The **SDP** (**service discovery protocol**) defines actions for both servers and clients of Bluetooth services. The specification defines a service as any feature that is usable by another (remote) Bluetooth device. A single Bluetooth device can be both a server and a client of services. A SDP client communicates with a SDP server using a reserved channel on an L2CAP link to find out what services are available. When the client finds the desired service, it requests a separate connection to use the service. The reserved channel is dedicated to SDP communication so that a device always knows how to connect to the SDP service on any other device. A SDP server maintains its own SDP database, which is a set of service records that describes the services the server offers. Along with information describing how a client can connect to the service, the service record contains the service's UUID, or universally unique identifier.

3.5. Comparison between bluetooth and other wireless communication technologies

Bluetooth is not the only short range technology to cut the cable, other wireless technologies like WLAN, ZigBee and UWB will compete with Bluetooth in the market. The techniques of these technologies and their key application areas are summarised in Table 2. From the table, the strength and weakness of Bluetooth technology can be easily identified. This also gives a quick view on which wireless technology to be selected while developing wireless solutions.

3.6. Bluetooth security

Since security is one of the biggest concerns in healthcare, it will be particularly discussed in this section.

Table 2
Comparison of wireless technologies

	Frequency range (Hz)	Range (meter)	Maximum Speed(bps)	Power Requirement	Modulation	Network	Application Focus
Bluetooth	2.4 G	10/100	3 M with EDR	low	FHSS	P2P	Cable replacement
ZigBee	2.4 G	10–100	250 k	low	DSSS	Mesh	Sensor network, monitoring
UWB	3.1–10.6 G	10	500 M	Low	OFDM or DS-UWB	P2P	Video/audio data
WiFi b	2.4 G	90	11 M	High	DSSS	IP & P2P	LAN, Internet
a	5 G		54 M				
g	2.4 G		54 M				
WiMAX	10–66 G	50 k	70 M	High	QAM	IP	Metro area broadband Internet connectivity
WiBro	2.3–2.4 G	1–5 k	30–50 M	High	QPSK	IP	wireless broadband Internet
Infrared		1 m	9.6 k–16 M		OOK/PPM/ Subcarrier	P2P	Remote control
RFID	Low: 100–500 k	Short-medium	Low		backscatter	P2P	Access control, Animal identification, Inventory control, Car immobiliser
	Medium: 10–15 M	Short-medium	Medium				Access control, Smart cards
	High: 850–950 M 2.4–5.8 G	Long	High				Railroad car monitoring, Toll collection systems
NFC	13.56 M	20 cm	106k/212k/424k	low	backscatter	P2P	Ticketing, payment, gaming
802.20	3.5	15 k	1 M	high	OFDM	IP	Mobile Broadband for mobile users

Bluetooth specification defines the security measures at both application layer and link layer. At link layer four different entities are used for maintaining security: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be generated for easy new transaction.

The Bluetooth address is a unique 48-bit physical address imprinted on the chip by the manufacturer. It can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. The size of the authentication key is always 128 bits. The size of the encryption key varies between 8 and 128 bits. The encryption key is entirely different from the authentication key, although the latter is used when creating the former. Each time encryption is activated, a new encryption key shall be generated. Thus the lifetime of the encryption key does not necessarily correspond to the lifetime of the authentication key.

Pseudo-random numbers are used to generate authentication and encryption keys. It should not be repeated and randomly generated.

These security measures have been maintained by Key Management, Device Authentication and Packet Encryption.

Key Management Key management offers following three ways to implement security

Firstly using a four digit personal identification number (PIN) that is generated by user or the device. Secondly for authentication Bluetooth uses one private link key among four authentication keys that includes a unit key (is generated by single Bluetooth device), combination key(generated by two Bluetooth devices), master key(generated by master device in piconet to send massages to all devices) or an initialization key(is used to provide security during device initialization process). The third is to use a private encryption key that is derived from the link key in use to authenticate it again with the second device. The private encryption key varies in length from 8 bit to 128 bits.

Apart from the above keys each Bluetooth device has its own unique 48 bit address assigned by Institute of Electrical and Electronics Engineers(IEEE). While generating secret keys device address is also used as a part of the key.

Device Authentication For device authentication a protocol checks that the two devices engaged in the communication process know the symmetric key. If both know the key the authentication process is successful, otherwise it fails.

Packet encryption Packet encryption is dealt via three encryption modes. In the first mode there is no encryption, in second mode packets are encrypted only between two devices and in one to multiple devices communication packets are not encrypted, in third mode all packets are encrypted.

4. Applications of bluetooth technology in healthcare

Based on its two connection types, point-to-point and point-to-multipoint, two typical examples of application of Bluetooth technology in healthcare will be described. One is the mobile diabetes management system developed at Kingston University [4]. The other is the EU project MobiHealth [18].

Mobile Diabetes Management System (MDMS) developed at Kingston University provides a mobile environment to access the diabetes management service for diabetics and healthcare personnel. It offers a wireless solution via Bluetooth and GPRS. The system architecture is shown in Fig. 3.

In this system, there are four user groups: diabetic, physician, medical administrator and system maintainer. The application of Bluetooth is on patient's side. A Bluetooth module is integrated in the blood glucose meter. The meter is connected to the Bluetooth enabled mobile devices like mobile phone and PDA (Personal Digital Assistant). While the blood glucose is measured, the data is stored in the

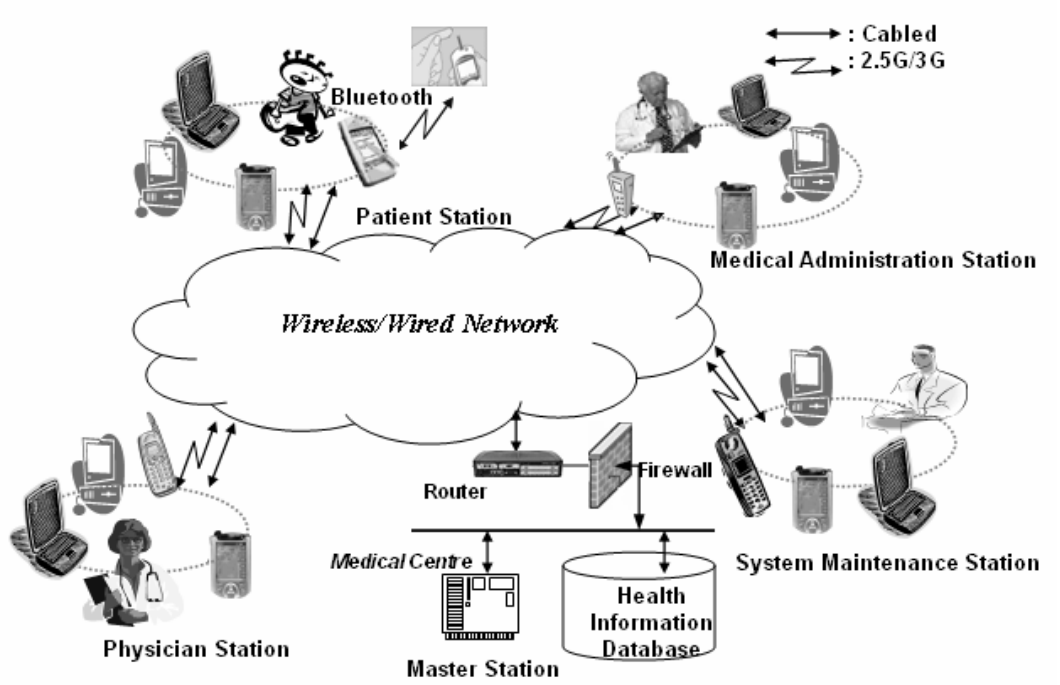

Fig. 3. System architecture of the mobile diabetes management system.

meter. After the connection of the Bluetooth, the data will be transmitted to the mobile device and then to the server on medical center via GPRS.

The motivations of application of Bluetooth in automatic transmission of the blood glucose data have been driven by both patients and medical professionals. Traditionally the blood glucose is read by the patient and written on a piece of paper. The paper will be brought to the nurse when the patient visits the clinics. The nurse will then examine the data for considering further medication and put the data into database for the record. This process is time consuming, waste of paper and causing mistakes. The most important is the nurse can't monitor the conditions of the patient continuously and adjust its medication plan in case of any abnormal situations. The wireless instant transmission of the data can make sure the genuineness of the data and overcome the limits mentioned above so as to provide a better service.

Several issues have been considered while applying Bluetooth technology in this application: connection, user interface, and security.

4.1. Connection

The mobile phone is the active party to call data from the glucose meter. There are several stages to connect the Bluetooth enabled glucose meter and the mobile phone:

– Search and identify the relative Bluetooth enabled glucose meter. The data acquisition software will search all the available Bluetooth devices at first time. The user can then specify the desired device to be connected. The Bluetooth address of the meter will be saved locally within the mobile phone after a successful pairing. Afterwards, it is not necessary to go through this stage and the meter will connect to the mobile phone automatically.

- Build Bluetooth connection channel. This means the data acquisition software has found the specific Bluetooth sensor, and try to build the communication channel for data transmission.
- Reading data. As soon as the Bluetooth communication channel is built, the data acquisition software will send command to inform the glucose meter to transmit data. If it is a legal command, the meter will be ready to transmit the data saved in the meter.
- Close the Bluetooth connection. When the data acquisition software receives indication of the end of data, the software will close the Bluetooth connection to save energy.

After the data from the meter is received, some other processes will be performed on mobile:

- Initial data processing. The data will be processed before sending it to the medical control centre. The reasons are: (1) filtering the useless data since not all the data received are the measurement; (2) first-hand data analysis. The software will tell user immediately if the measurement is too high or too low according to the predefined medical rules; (3) uniform the format of data to be sent to the medical centre to alleviate the load of the master station.
- Send data to the medical control centre. The software will initiate the GPRS or 3G connection to send data through Internet to the medical centre.
- The master station sends the analysis result and possible medication change to the patient station.

4.2. Security

Several security measures have been implemented in this system to protect the privacy and confidentiality of the patient. This includes:

Authentication and authorization MDMS will check the identification of the patient station before a patient can submit data to the medical control centre. A dialog prompts the user for his or her ID and password for verification. This account information is sent to the medical control centre for validation. If it is invalid, the patient station will not be able to send the data to the medical centre. Otherwise, the account information will be stored to avoid the repetition of the operation. Now the patient station is ready to collect and send the data from the sensor to the medical control centre.

Access control After the user's identification is confirmed, the system will also check the user's rights on each operation. Meanwhile, only the functions within a MDMS user's privilege range are listed. MDMS user management provides the functionalities to grant user's privilege to access other MDMS services. The access to the database is also controlled.

Prevention of invalid input The validity of the inputs will be checked in MDMS before further data analysis. If a wrong data input is attempted, the warning message will be prompted to the user along with the correct format or interpretation of the data.

Security of data transmission MDMS adopted SSL(Secure Sockets Layer) for secure data transmission.

4.3. MMI

The software is developed using Java language to make it universal operatable on different operating systems. It has a simple MMI so that users can operate easily on mobile devices. Figure 4 shows the MMI of user management on Sony Ericsson P800 mobile when a user logs into MDMS as a medical administrator. In addition XML (eXtensible Markup Language) is used to format the data to make it portable. Thus the system is portable and universal accessible.

This is the typical application of Bluetooth as a point-to-point link in healthcare. The same infrastructure can be used in monitoring other vital signs and managing other medical conditions, such as ECG

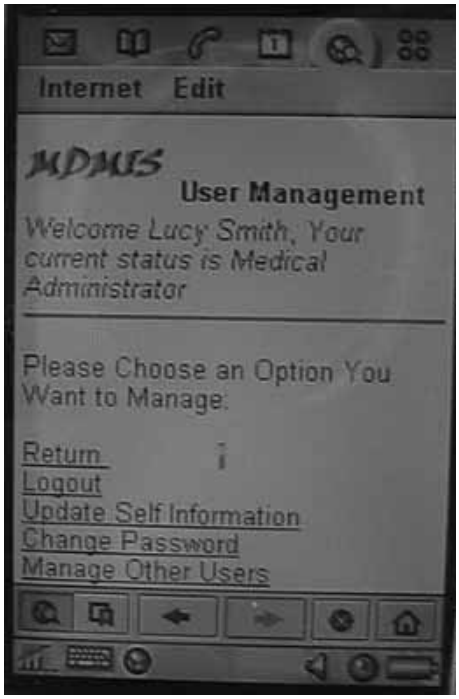

Fig. 4. User interface of MDMS.

monitoring [20], medication consumption monitoring [21], peak flow meter [22], weight, blood pressure, thermometer, stethoscopes [23].

The gateway of transmitting the data to the remote center can be mobile devices via mobile communication like above example, it can be also wired network like Internet and PSTN [24]. In addition, the signal from medical sensor can be modularized for future upgrade by modifying the software [11].

However, the concerns are still there. For example the security of MDMS, although several security measures have been implemented, no security regarding to the Bluetooth transmission is applied. The inherent limit of the security of Bluetooth technology was not addressed.

Next is the example of application of Bluetooth in piconet in healthcare. MobiHealth is a research project supported by the EU. The system is based on the concept of the body area network (BAN). It's highly customizable allowing sensors to be seamlessly connected and transmit the monitored vital signs.

The system's architecture is shown in Fig. 5. It consists of sensors, actuators, communication and processing facilities. Communication between entities within a BAN is called *intra-BAN* communication. Sensors and actuators establish an ad-hoc network. To use the BAN for remote monitoring, external communication is required which is called *extra-BAN* communication. The gateway that facilitates extra-BAN communication is the *Mobile Base Unit* (*MBU*) which can be any device with sufficient processing power capable of managing the BAN and providing extra-BAN communication services.

Figure 6 shows the functional architecture of the service platform. The dotted square boxes indicate the physical location where parts of the service platform will be executing. The rounded boxes represent the functional layers of the architecture.

The M-health service platform consists of sensor and actuator services, intra-BAN and extra-BAN communication providers and an M-health service layer. The intra-BAN and extra-BAN communication providers represent the communication services offered by intra-BAN communication networks and

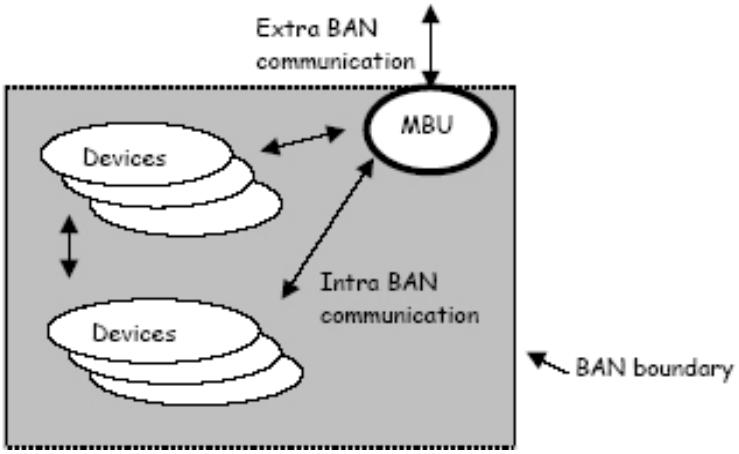

Fig. 5. MobiHealth BAN architecture.

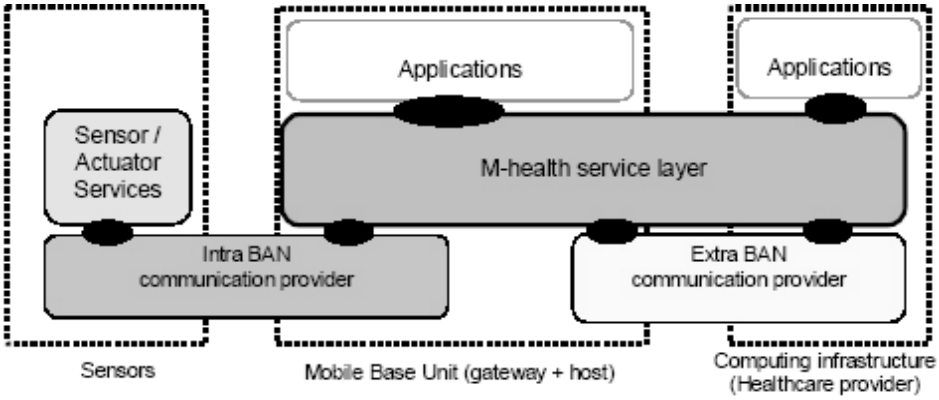

Fig. 6. MobiHealth Service platform functional architecture.

extra-BAN communication networks, respectively. The M-health service layer integrates and adds value to the intra-BAN and extra-BAN communication providers. The M-health service layer masks applications from specific characteristics of the underlying communication providers, such as the inverted consumer-producer roles.

The piconet software BANip has been implemented using Java 2 Micro Edition (J2ME) on the MBU as an HTTP client that collects a number of samples into the payload of an HTTP POST request and invokes the post on the surrogate. A standard HTTP proxy was used to act as a security gateway of the surrogate. In case the surrogate needs to control the MBU, these control commands are carried as payload of the HTTP reply.

The surrogate has been implemented using the Jini Surrogate architecture. Jini provides the implementation for auto-discovery and registration of the BAN. Other components, such as the BAN data storage component, are service users from the perspective of the surrogate.

The MobiHealth has the capability of measuring six different signals: ECG, Pulse Oximetry, Temperature, Marking, Respiration and Motion/activity. The signals can be visualized on the MBU and were sent to the healthcare organization where it can be reviewed by medical personnel.

MobiHealth has more power than some purpose built system like MDMS and can be used in wider range in healthcare sector. The trailed applications include:

- Telemonitoring of patients with cardiac arrhythmia.
- Integrated homecare for women with high-risk pregnancies.
- Tele trauma management.
- Support of home-based healthcare services.
- Outdoor patient rehabilitation.
- Lighthouse alarm and location.
- Physical activity and impediments to activity for women with RA.
- Monitoring of vital parameters in patients with respiratory insufficiency.
- Home care and remote consultation for recently released patients in a rural area.

MobiHealth is the typical application of Bluetooth via point-to-multipoint link. Other systems like CodeBlue [25] and [7] have the similar infrastructure and functionality.

5. Considerations of bluetooth application in healthcare

Bluetooth provides the convenience as a cable replacement. However, Bluetooth has limitations and not all the cables can be replaced. Some considerations have to be kept in mind while developing Bluetooth applications, including:

- Connection time.
- Interference.
- Security.
- Size of the network.
- Power consumption.
- Man-machine interface (MMI).
- Bandwidth Constraints.

5.1. Connection time

It's mentioned above that Bluetooth device can't connect instantly. It can take up to 10.24 seconds to discover a Bluetooth device. The long connection time is a limitation for some applications, such as "panic button".

5.2. Interference

Bluetooth is working in ISM frequency band sharing with other wireless technologies. It's prone to the interference caused by those wireless technologies and other resources. The radio link between Bluetooth devices can never be guaranteed. Thus Bluetooth technology should not be used for safety-critical applications where data absolutely must get through.

5.3. Security

Security for Bluetooth is provided on the radio paths, that link authentication and encryption are provided. However, there are still number of weaknesses and vulnerabilities in the security system and

the true end-to-end security is not possible without providing security solutions for the higher layers of Bluetooth.

Some of the known problems with Bluetooth security can be summarised as [26]:

- Pseudo random number: The pseudo-random number generator is unspecific. The generator may produce static numbers or periodic numbers which could be a problem as it may affect the authentication scheme.
- Short PIN: The PIN key is short, hence it can be easily guessed. Intruderscan easily compute the correct link from shorter PIN key compared to longer PIN key where the calculation will be more complexe.
- Unit key: The unit key is reusable and becomes public once used. It is better to use a key set instead of only one unit key. The problem is that the unit key may be used in encryption.
- Master key: The master key is shared. Changing the broadcast scheme can solve this problem.
- User authentication: The authentication service is supported for devices but not for users. Malicious users with stolen devices can access the network resources and services without trouble. Employment application level security and user authentication is required.
- Device authentication: The attempts for authentication are repeated. Bluetooth SIG needs to develop a limit for authentication features to prevent unlimited request. Also, the entry number of the list should be limited.
- $E0$ stream cipher: The $E0$ stream cipher algorithm is weak, and it can be guessed. A better encryption procedure is needed.
- Key length: The key length is negotiable. The encryption may abort. There should be a global agreement on minimum key length.
- Mutual authentication: One way challenge-response authentication can be attacked using the man-in-the-middle attack. Mutual authentication is required.
- End-to-end security: Security services are for the wireless link only, not end-to-end, therefore additional security measures at higher layers need to be implemented.

5.4. Size of the network

Bluetooth has the capability to support only up to seven Bluetooth devices in a single network. It's not suitable for monitoring complicated system with more than seven parameters at a single time.

5.5. Power consumption

Since most Bluetooth devices are mobile and use battery power, it is essential to conserve power. The Bluetooth specification has various methods for achieving low power consumption. One scheme allows the devices to adjust the power depending on the range of communication. The lower power level covers a distance of about 10 meters while the higher power level can cover about 100 meters. A second method of power saving allows a device to alter power consumption depending on its activity to either active, sniff, hold, or park mode. The third method of reducing power consumption deals with dynamically regulating the transmitted power. If the receiver signal strength indication (RSSI) of a device varies from its optimal value, the device can request an increase or a decrease of the other device's transmitted power. The device receiving the request may then alter its output accordingly.

Recently many companies unveiled the Bluetooth solutions either as a chipset or a single chip. However, most of the current Bluetooth solutions require more power than the Bluetooth specification [27]. This requires the adoption of power optimisation techniques to prolong the life of the battery.

5.6. Man-machine interface (*MMI*)

Most of the patients are elderly. They prefer a simple and straightforward way to operate on the medical device. The MMI must be simple to use, simple to set up, and simply it must be simple.

5.7. Bandwidth constraints

Bluetooth was developed as a low-bandwidth, wireless connectivity solution. It's important to keep the bandwidth constraint in mind when designing your application. For specification version 1, the bandwidth is 720 kbps. This means that there are 720 kbps available to be shared among *all* connections on a link. When an application assumes that all 720 kbps are available to a single connection, the performance of the connection will be degraded, or the application is likely to experience a much lower level of throughput.

With the latest development of specification version 2, the date rate can reach 3 Mbps with enhanced data rate (EDR). However this is still not enough for transmitting medical images and videos in real time. The bandwidth constraints still exist. While designing Bluetooth application, it is important to scrutinise the application's bandwidth and throughput need.

6. Challenges and future of bluetooth in healthcare

Bluetooth technology has a few drawbacks, including vulnerable security, relatively short range, low bandwidth, prone to interference, and supporting limited-sized personal area network. These drawbacks limit its wide application in healthcare as well as other areas.

With more people and devices are moving toward wireless, Bluetooth has to compete or coexist with other wireless technologies, such as Wireless LAN, WiMAX, UWB, and ZigBee. The drawbacks need to be resolved for a wide market in the future. Based on the characteristics of the medical environment and the special requirements, the following issues will have to be addressed in the future development of Bluetooth technology in healthcare.

Bandwidth: As a short range wireless technology, Bluetooth is usually working with other wired or wireless technologies to form the networking. The low bandwidth will produce a bottleneck in the network. The good news is this problem could be solved very soon. In May 2005, SIG announced its intent to work with developers of UWB to develop a next-generation Bluetooth technology using UWB technology and delivering UWB speeds. This will enable Bluetooth technology to be used to transfer medical images and video to expand the applications.

Bluetooth personal area networks: As the example showed above, personal area network has powerful and flexible applications in healthcare. Bluetooth was specifically designed for use in this fashion and widely used nowadays. But the size of the Bluetooth supported personal area network is limited. As of now, there is no protocol for using Bluetooth as a large personal network, though the protocol is being researched.

Security: security is becoming more and more important, particularly to the healthcare. The vulnerable security of Bluetooth technology and the security in personal network need to be enforced.

7. Conclusion

This paper gives an insight review of application of Bluetooth technology in healthcare. Owing to its convenience to cut the cable, it's widely used in healthcare, particularly very popular in monitoring

patients away from medical environment. However, Bluetooth has some limitations, such as vulnerable security, long connection time, prone to the interference, low bandwidth and its incapability to support large personal area networks. This limits its application in particular area, such as emergency care and medical images transmission. These issues shall be investigated in the future to meet the requirement of medical care.

References

[1] Radio News, April 1924.
[2] R. Bashshur and J. Lovett, *Assessment of Telemedicine: Results of the Initial Experience*, Aviation Space and Environmental Medicine, January 1, 1977, 65–70.
[3] R.S.H. Istepanian, E. Jovanov and Y.T. Zhang, 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* **4** (2004), 405–411.
[4] Y. Zou, R.S.H. Istepanian, X.H. Wang and T. Geake, Design and Implementation of Universal Mobile Diabetes Management System, *Journal of Mobile Multimedia* **4** (2006), 273–284.
[5] K. Oyri, I. Balasingham, E. Samset, J.O. Hogetveit and E. Fosse, Wireless continuous arterial blood pressure monitoring during surgery: a pilot study, *Anesth Analg* **2** (2006), 478–483.
[6] C.W. Mundt, K.N. Montgomery, U.E. Udoh, V.N. Barker, G.C. Thonier, A.M. Tellier, R.D. Ricks, R.B. Darling, Y.D. Cagle, N.A. Cabrol, S.J. Ruoss, J.L Swain, J.W Hines and G.T. Kovacs, A multiparameter wearable physiologic monitoring system for space and terrestrial applications, *IEEE Trans Inf Technol Biomed* **3** (2005), 382–391.
[7] J. Yao, R. Schmitz and S. Warren, A wearable point-of-care system for home use that incorporates plug-and-play and wireless standards, *IEEE Trans Inf Technol Biomed* **3** (2005), 363–371.
[8] J. Seo, J. Choi, B. Choi, D.U. Jeong and K. Park, The development of a nonintrusive home-based physiologic signal measurement system, *Telemed J E Health* **4** (2005), 487–495.
[9] Y. Jasemian and L. Arendt-Nielsen, Evaluation of a realtime, remote monitoring telemedicine system using the Bluetooth protocol and a mobile phone network, *J Telemed Telecare* **11** (2005), 256–260.
[10] J. Yousef and A.N. Lars, Validation of a real-time wireless telemedicine system, using bluetooth protocol and a mobile phone, for remote monitoring patient in medical practice, *Eur J Med Res* **6** (2005), 254–262.
[11] M.F. Rasid and B. Woodward, Bluetooth telemedicine processor for multichannel biomedical signal transmission via mobile cellular networks, *IEEE Trans Inf Technol Biomed* **1** (2005), 35–43.
[12] P. Rubel, J. Fayn, G. Nollo, D. Assanelli, B. Li, L. Restier, S. Adami, S. Arod, H. Atoui, M. Ohlsson, L. Simon-Chautemps, D. Telisson, C. Malossi, G.L. Ziliani, A. Galassi, L. Edenbrandt and P. Chevalier, Toward personal eHealth in cardiology. Results from the EPI-MEDICS telemedicine project, *J Electrocardiol* **4** (2005), 100–106.
[13] http://www.bluefishrx.com/, accessed on 15$^{\text{th}}$ March, 2006-3-17.
[14] H. Qian, P.C. Loizou and M.F. Dorman, A phone-assistive device based on Bluetooth technology for cochlear implant users, *IEEE Trans Neural Syst Rehabil Eng* **3** (2003), 282–287.
[15] Specification of the Bluetooth System, Version 2.0 + EDR[Vol 0], 4 Nov. 2004, Bluetooth Document, http://www.bluetooth.com/.
[16] http://www.bluetooth.com/Bluetooth/Learn/Security/, access on 15$^{\text{th}}$ March 2006.
[17] Y. Zou, X.H. Wang, R.S.H. Istepanian and N. Philips, *Bluetooth Connectivity Issues on M-health Application*, WPMC'05, Sep, Aalborg, Denmark, 2005.
[18] K. Wac, R. Bults, D. Konstantas, A.V. Halteren, V. Jones, I. Widyi and R. Herzog, *Mobile Healthcare Over 3G Networks: the MobiHealth Pilot System and Service*, Global Mobile Congress, Shanghai, 2004, 11–13.
[19] http://www.mobihealth.org/, accessed on 15$^{\text{th}}$ March 2006.
[20] http://www.wirelessecg.com/, accessed on 15$^{\text{th}}$ March 2006.
[21] M. Lampe, M. Strassner and E. Fleisch, *A Ubiquitous Computing Environment for Aircraft Maintenance*, ACM Symposium on Applied Computing 2004, Nicosia, Cyprus, March 14–17, 2004.
[22] http://www.corscience.de/en-diagnosis.html, accessed on 15$^{\text{th}}$ March 2006.
[23] http://www.lifesourceonline.com/and med.nsf/index, accessed on 15$^{\text{th}}$ March 2006.
[24] Wireless telehealth PSTN gateway, RTX document, http://www.rtx.dk/Default.aspx?ID=118, accessed on 15$^{\text{th}}$ March 2006.
[25] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton, *Codeblue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care*, Proc. Intern. Workshop on Wearable and Implantable Body Sensor Networks, 2004. April 6–7 2004, Imperial College London, United Kingdom.

[26] O. Khalif, *Security in Bluetooth Technology*, Postgraduate Essay, African Institute for Mathematical Sciences, 8 June 2005.
[27] M. Ziegler, *An Overview of Bluetooth: Architecture, Power Consumption and Performance*, report, University of Virginia, http://www.ece.virginia.edu/~mmz4s/papers/ECE613project bluetooth.pdf, accessed on 15th March 2006.

Xinheng Wang is a senior lecturer in mobile computing at Faculty of Computing, Information Systems and Mathematics, Kingston University, UK, with research interests in low power wireless networking in healthcare, intelligent chronic disease management, and network condition monitoring. He has published more than 30 papers on these topics on international journals and conferences.

Muddesar Iqbal is a research PhD student at Faculty of Computing, Information Systems and Mathematics, Kingston University, UK, with research interests in wireless PAN networks and software development for web applications. He is also lecturing in Boston College London.