A Practical U-Healthcare Network with Security and QoS[1]

Shiow-Yuan Huang[1], Cheng-Chan Hung[2], Cheng-Chi Lee[1,3]
[1]Department of Photonics & Communication Engineering
Asia University, No.500, Lioufeng Road
Wufeng Shiang, Taichung, Taiwan, R.O.C.
syhuang;cclee@asia.edu.tw

[2]Department of Computer Science & Information Engineering
Asia University, No.500, Lioufeng Road, Wufeng Shiang
Taichung, Taiwan, R.O.C.
cctks.hung@msa.hinet.net

[3]Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City
Taipei County 24205, Taiwan, R.O.C.
cclee@mail.fju.edu.tw

Journal of Digital Information Management

ABSTRACT: *As a consequence of rapid technological development, the normally isolated medical sensor platform is gradually being integrated into networks. However, most ubiquitous or mobile health systems are lacking a system that combines both network security and QoS (Quality of Service). This paper investigates the possible security and QoS methods of a ubiquitous healthcare network platform in OSI (Open System Interconnections)-layers. This network platform is based on the Wireless Overlay Networks (WON) Bluetooth, 802.11 and 802.16 over IPv6 network, and provides a secure and stable U-healthcare platform by including the application of healthcare sensors with RFID, U-healthcare PDA, VoIPv6, falling detection, and patient orientation.*

Categories and Subject Descriptors
C.2.1[Network Architecture and Design]; Wireless communication: D.4.6 Security and Protection

General Terms: Healthcare, Network Security, IPv6 Network

Keywords: IPv6 network, Healthcare, Security, QoS, Ubiquitous

Received: 8 October 2010, Revised 12 November 2010, Accepted 20 November 2010

1. Introduction

As a consequence of the developments of science and technology, medical sensing technology is evolving from the previous electronic care (e-care) to the ubiquitous care (U-care). Government promotion of a U-Taiwan plan indicates the coming of the ubiquitous society. What is meant the Ubiquity? It means mobility of sensor networks, security, standard, integration (health system, service model), and CAD (Computer Assisted Decision). This paper studies the above-mentioned characteristics of the Ubiquitous technology.

As shown in Figure 1, security covers the scope of the whole system, and QoS covers 80%. Therefore, security and QoS will be the very important in the U-healthcare system. However, most of the ubiquitous health systems [1], [2], [3], [4], [5] have not yet proposed a system with both network security and QoS. In this paper, we will use the existing security mechanisms and methods of QoS to achieve the needs of U-healthcare network.

In addition, we use the advantages of ubiquity of IPv6, such as large address space, an extension of encrypted authentication, quality of service, enhanced ability to address, mechanisms to simplify the header format to this system. The Internet of the future will support the basic features with multimedia, security and mobility. IPv6 is fully equipped with the above-mentioned features and the ability of ubiquity. Therefore, IPv6 will be the best choice for the next generation Internet protocol, which is being applied to U-life and to the way of ALL-IP.

This paper studies a U-healthcare network platform with security and QoS. The use of the new IPv6 security features and QoS options improves the environment of the U-healthcare network by not only sharing the cost of healthcare and human resources, but also by being a long-term monitor of unusual health symptoms. The U-healthcare environment will be the primary defense for medical care, safety and the health of human beings. A U-healthcare environment with security and quality of service is needed for our development.

The remainder of the paper is organized as follows. We describe the U-healthcare network demand and problems encountered in Section 2. In Section 3, we review the properties of IPv6 and describe our implementation of the system, with security and QoS. In Section 4, we present the test system design with IPv6. Finally, Section 5 concludes the paper.

Figure 1. The relevance between Ubiquitous and WON (Wireless Overlay Network)

[1]Responsible for correspondence: Dr. Cheng-Chi Lee; E-mail: cclee@mail.fju.edu.tw.

2. U-healthcare Network Demand

Along with social and economic development, medical advances have enabled people to increase their life expectancy, with the consequent gradual aging of the population. The problem of an aging population will need urgent attention in the 21st century. The increasing demand for elderly health care is the most pressing current need and will continue to in the future. Therefore, to consider the increasing demand for elderly healthcare as well as mobile care, it is necessary to establish a new type of healthcare system, one with a network technology to provide U-care services. When a person has urgent need of heath care, the U-healthcare system issues an immediate warning through the network, so that the healthcare workers will be able to locate the person quickly and efficiently and give the necessary emergency treatments.

Compared to the current IPv4 networks, IPv6 is the next generation Internet protocol and has many new features, such as large address space, Internet operations support, an extension of the encrypted authentication mechanism, enhanced addressing capabilities, automatic addressing mechanism, simplification of the header format, and so on. Based on the above advantages, this paper chooses IPv6 as a U-healthcare network protocol. As the U-healthcare network has a large number of sensor nodes, the transmission network will be the limiting factor for transmission quality. It must also be borne in mind that wireless networks have problems of network security. The following describes some of problems of the U-healthcare network.

2.1 Problem of Large Sensor's IP Space Requirement

The U-healthcare system for each of the care-givers has a number of sensor nodes (ex. heart rate, blood pressure, body temperature, respiration, ECG, EEG, a fall position). IP space for the sensor nodes in the existing IPv4 network is not enough. Therefore an IPv6 network should be used to allow each sensor to have a unique IP address. The public IP will have direct links to various sensing networks and facilitate the application of remote services in the future.

2.2 IP Auto-Configuration Issue

In a general IPv4 network, auto-configuration IP is necessary in the DHCP server environment. IPv6 with stateless auto-configuration ability does not need a DHCP server in the network. It has a link-local IPv6 addressing function which provides IP connection and solves the sensor's addressing problems in a mobile environment.

2.3 Normal QoS Issue

Among the ubiquitous nodes there is a variety of different network environments, in particular the provision of healthcare information transmission networks. Therefore, QoS is an important issue.

QoS is provided in many ways, traffic policing, Integrated Services (IntServ), Differentiated Services (DiffServ), Resource Reservation Protocol (RSVP) and Multiple Protocol Label Switch (MPLS), to achieve the purpose of providing reliable and effective transmission. For example, in the extension field of IPv6 packets, there are two headers to be used to mark the transfer QoS priorities, namely routing header and Hop-by-Hop header. IPv6 with a unique flow label can work with Multiple Protocol Label Switch (MPLS), a different information flow corresponding to the different flow label to control the quality of service. No doubt, IPv6 provides the best QoS functionally for a U-healthcare network protocol.

2.4 Emergency QoS Issue

Several papers [6], [7] have discussed the healthcare system implementation. Although they have provided the novel architecture of e-home-care and the telemedicine function, they have failed to consider the actual delivery issue of the healthcare system, especially on the impact of U-home-care network after adding the multimedia streaming. Secondly, in providing QoS telemonitoring perspective, such as the paper [8] and [9], the main approach is to divide the sensor obtained data into two categories: periodic reporting data, and unpredictable emergency data; and then guarantee to upgrade the emergency data transmission through algorithm. This mechanism mainly guarantees the QoS used between the client and access point (AP). In paper [10] quantifies QoS levels depending on available resources. Another example is paper [11] mentioned in this paper. It uses the algorithm of optimized rate control medical video stream system to satisfy the relevant m-QoS requirements in 3G networks, thus providing the health telemonitoring system with even better transmission efficiency in video stream transmission.

2.5 Hand off and Roaming Issue

In a large-scale mobile sensing system it is necessary to consider hand off at sensing and roaming. Mobile IP provides a mobile node mobile transmission function. The base IPv6 protocol supports mobility more naturally than IPv4 [12], [13].

2.6 Security Problem

When a sensor node connects to the Internet from the front of the sensor nodes, there is the issue of network security such as: the security problem in PAN's Bluetooth, WLAN's 802.11 series, WAN, Internet, and all network levels. These are the problems that the construction of a U-healthcare network must consider. Therefore, this paper mentions these security issues and healthcare demands, through the research of security-related technology. And we also refer to related with IPv6 security paper [14], real-time monitoring system paper [15] and challenges of security in health care applications [16], to accomplish this practical U-healthcare system.

2.7 Translation Problems with IPv6 and IPv4

Judging from the current RFC (Request For Comment) on IPv4/IPv6 transition aware of the document, the main methods of translation will be available as follows:

- Dual Stack (RFC 1933)
- Tunneling (RFC 1933, 3056, 3053)
- Translator (RFC 2765, 2767, 3089, 3142)

Demand of U-healthcare Network	Feature of IPv6
A large number of biomedical Sensors	Large IP space
Sensor's IP automatically	Stateless auto-configuration
Real-time transmission	QoS functions
Sensors hand off and roaming	Mobile IPv6
Bio-medical information on internet	IPSec, AH, ESP
IPv6 and IPv4 translation	Dual stack, tunneling, translator

Table 1. U-healthcare demands and characteristics of IPv6

Due to the current lack of popularity of the IPv6 network, it is difficult to have a comprehensive IPv6 network on the

Internet. Considering the advantages of an IPv6-based network, this paper will build the IPv4/IPv6 network with a dual stack base. So that IPv6, through an IPv4 network providing DNS resolution, will co-exist with an IPv4 network, and so improve network compatibility. Table 1 summary of the demand of a U-healthcare network and the solution which IPv6 provides.

3. U-healthcare Network with Security and QoS

Previously, improvements to the U-Healthcare system were based on wire-sensing systems. However, major problems were encountered, these were concerned with network security and the quality of service. About, network security and QoS there are many ways, but not all are suitable for a U-healthcare. Therefore, this paper follows the healthcare network platform's ubiquitous demand and designs the IPv6 U-healthcare network to achieve network security and quality of service and to integrate WON (WPAN, WLAN, WAN, and Internet) as well as remote application. It expects this system to provide a U-healthcare network platform with both security and quality of service for the care of the elderly.

3.1 The Structure of U-healthcare Network

First, the front sensors will be a new type of wireless sensor, designed to capture sensing information through a wireless personal area network (WPAN) application. This information will be forwarded using a PDA and a notebook with Bluetooth and 802.11 capabilities. The PDA/notebook, using the Wi-Fi network interface, transmits the information to the back-end web and database server as well as sending it to the healthcare database systems.

Finally, the Intranet will consist of the dual stack IPv4 and IPv6 networks. In remote locations hospitals, care centers, family, back-end management of health care centers and other units will be able to connect to the network.

The entire U-healthcare network platform architecture is show in Figure 2:

3.2 Authentication Security in Physical Layer and Data Link Layer

In the physical layer and data link layer, we use MAC authentication with hidden SSID. First, the sensor's MAC Address is configured on the AP, then pre-set to hide the AP SSID broadcast, and the pre-set the AP certified connection password on it.

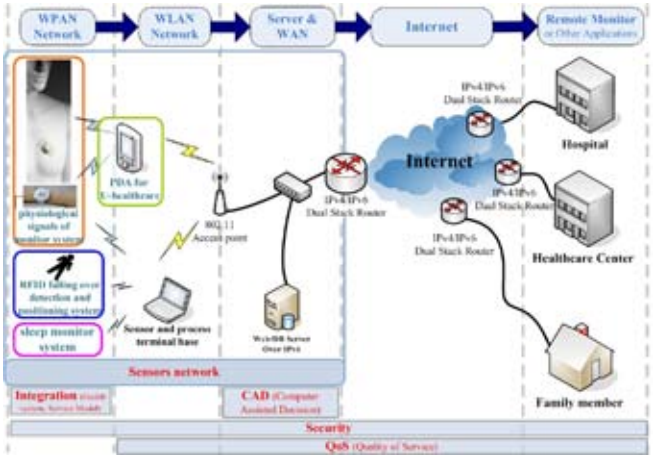

Figure 2. The structure of U-healthcare system and wireless overlay network

After the completion of the above steps, the AP will set up a connect profile. Thus the network can login only following the profile. The security set steps are as follows:

1. Hide AP SSID broadcasting
   To prevent non-U-healthcare network equipment searching for an AP
2. Connect AP using EAP 128bit encryption
   To prevent any client from connecting to the U-healthcare AP
3. Clients were connected to the AP using MAC address authentication
   The MAC address has to be entered before the AP can be accessed.

When a sensor completes the above three steps, it can connect to the AP and access the U-healthcare network. The process is shown in Figure 3.

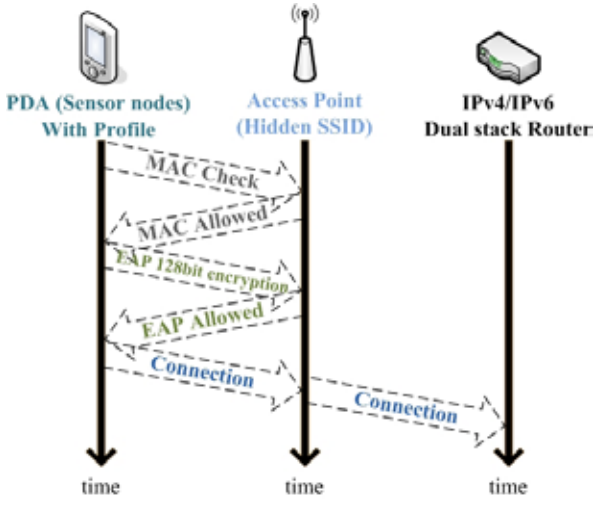

Figure 3. Process of U-healthcare network data link layer security certification

3.3 Network Layer Security

Though the IPv4 can provide security through network layer security protocol IPSec (IP Security), management and setup are an additional burden. For this reason, the design of IPv6 has taken into consideration the network security features, with the purpose of providing point-to-point embedded security capabilities. The use of next header in the authentication header and encrypted security payload header on the transmission of data encryption and authentication provides IPv6 users without the need of additional equipment or software to be able to achieve the effectiveness of network security.

3.3.1 Combined AH and ESP to Provide Integrity of the Data Encryption and Authentication Security Protection

An authentication header (AH) uses a key to the hash algorithms to sign the packet for the whole packet (IP header and payload) to provide authentication, integrity and the protection of the ban on re-broadcast.

Because AH does not encrypt data, it does not provide confidentiality. Encapsulating Security Payload (ESP) provides confidentiality for the contents of IP, but not for the entire package in transparent mode. It is usually only protection for the IP, not for the IP header.

In this paper, through the combination of AH and ESP, the security features provide biomedical information to verify the

IPv4

IP header	IP payload (TCP segment, UDP message, ICMP message)

IPv6 + AH (Authentication Header)

IP header	**Authentication header**	IP payload (TCP segment, UDP message, ICMP message)

IPv6 + ESP (Encapsulating Security Payload)

IP header	**ESP header**	IP payload (TCP segment, UDP message, ICMP message)	**ESP trailer**	**ESP Auth trailer**

IPv6+AH+ESP

IP header	**Authentication header**	**ESP header**	IP payload (TCP segment, UDP message, ICMP message)	**ESP trailer**	**ESP Auth trailer**

Figure 4. IPv6 U-healthcare network with AH+ESP

source of the packet and contents of packets to encrypt, and so obtain complete security. A variety of packet headers are shown in Figure 4.

3.4 Design for Application Layer Security

In the back-end database server systems, in order to prevent leakage of biomedical sensing information and to protect personal privacy, we use RFID (Radio Frequency IDentification) technology. A RFID identification card can be employed if users want to connect to the U-healthcare web database to observe their own health information history, or hospital or nursing staff need to know their patient's medical history. A password is entered to allow access to the private personal information. The operation process is shown in Figure 5.

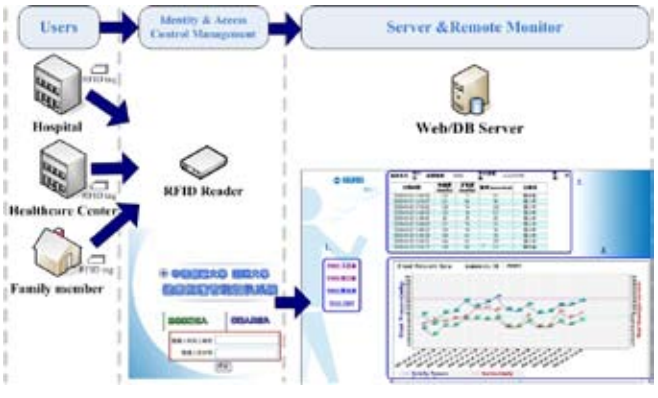

Figure 5. Application layer client application platform for information security certification process

3.5 Network Layer QoS in U-healthcare Network

In a U-healthcare environment, different data traffics with different classes of QoS requirements have to be transmitted simultaneously. But QoS is more complex than security. So we will only describe the IPv6's network layer characteristics for the main objectives of the discussion, and use a priority-based approach to achieve the purpose of QoS.

The header in the IPv6 packet has the two fields, namely traffic class and flow label. The priority level of the traffic class field divides into two main categories: *congestion-controlled* and *non-congestion-controlled*. Congestion control and non-congestion-control priorities and authority are divided into eight grades (Figure 6).

This paper proposes that the information is divided into two types of ubiquity, one packet of emergency information and the other measured by the sensor information packet, according to their respective fields, to give priority to control congestion in the shape of priorities 5 and 6 (Figure 6). This will protect the transmitting of the emergency information packets in the network congestion.

3.6 Transport Layer QoS in U-healthcare Network

In order to provide more protection for biomedical information transmission in our health care system, we propose the IPv6 layer 4 router multi-homing (RFC 4177) functions to provide *fault-tolerance* and *load sharing*.

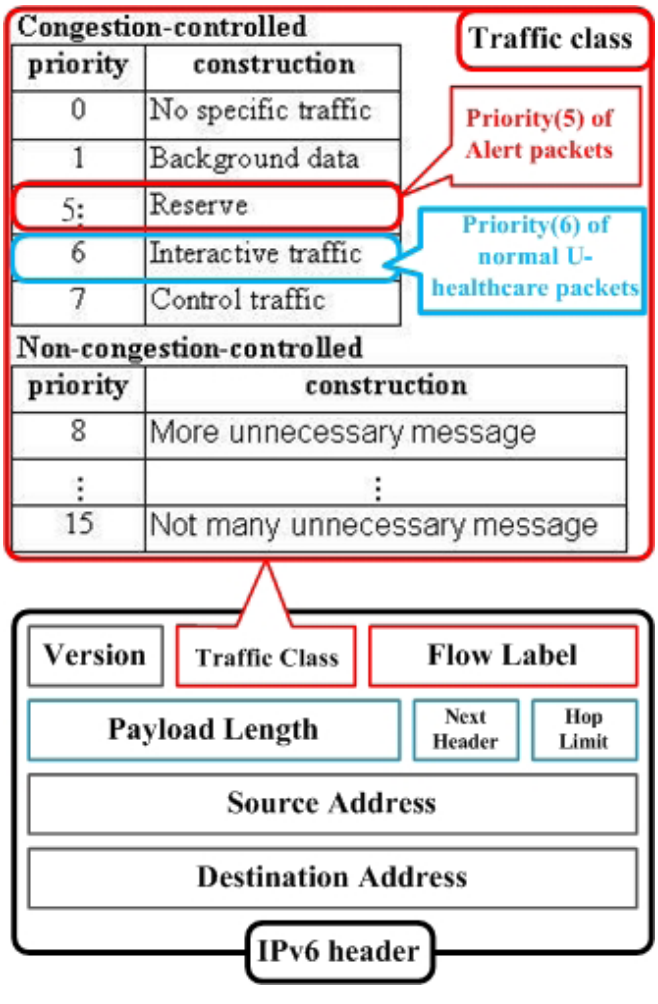

Figure 6. U-healthcare package priority in IPv6 traffic class field

Through the port routing rules in an L4 router, such as port 119 for the B line and other ports for the A line, we can use the A line for normal biomedical data transmission and the B line as a backup. When the A line is congested or disconnected, the B line will immediately take over the responsibility for information transmission or emergently data transmission.

Figure 7. IPv6 multi-homing with a layer 4 router

Finally, we organize the table of security and QoS as follows:

	Security methods	QoS methods
OSI-layer 7	Use RFID and Password to login the healthcare web site	
OSI-layer 4		Priority of Port Routing and Divergence path
OSI-layer 3	Combined AH and ESP to provide the data encryption and authentication security protection	Packet priority in Traffic class
OSI-layer 2	MAC filter	
OSI-layer 1	1. Hide AP SSID broadcasting 2. Connect AP using EAP 128bit encryption	

Table 2. Methods of secure and QoS in OSI-layer

4. Evaluations of Security and QoS

4.1 Security Evaluation

We use the security design of Section 3 and the basic security requirements to compare healthcare security methods with evaluation In Table 3.

Basic security requirements	U-healthcare security methods	Coincidence
Privacy	L7: RFID identity authentication L3: Transmission packet ESP L2:MAC filter L1: AP EAP 128bit encryption L1: Hide AP SSID broadcasting	Yes
Authentication	L7: RFID identity authentication L3: Transmission packet with AH & ESP	Yes
Non-repudiation	L7: RFID authentication for data writer	Yes
Integrity	L3: Transmission packet with AH & ESP for integrity check	Yes
Access Control	L2: MAC filter	Yes
Audit	L4: TCP provided connection-oriented transport	Yes

Table 3. Evaluation of basic security requirements

4.2 QoS Evaluation

The main purposes of the simulation results are to compare the general transmission of QoS mechanism through IPv6 traffic class QoS mechanism (packet priority in traffic class) to apply in the general families that commonly use the 10M/2M (fiber to the building) FTTB of Internet to go online, and the impact of IPv6 traffic class QoS effectiveness on network when it is congested. The simulation results are mainly divided into the following two categories to serve as the analysis basis.

1. Delay
2. Total packet loss rate

In data rate simulation test perspective, we select several commonly used emergency (vital) signals (digital sphygmomanometer, digital thermometer, respiration, heart rate and ECG) to work as the testing standards of TCP transmission. Other variable medical media: remote monitoring, ultrasound, cardiology, radiology, magnetic resonance image and digital radiography were then added in sequence simultaneously in order to understand the impact on network effectiveness while transmitting without the IPv6 traffic class QoS mechanisms. Table 4 is a list of medical data rates used in the simulation test.

Resolution (kbps/sample)	Number of patient	Total data rate
TCP (32)*	1	32 kbps
TCP (32)*	2	64 kbps
⋮	⋮	⋮
TCP (32)*	7	224 kbps
TCP (32)*	8	256 kbps
TCP (32)*	9	288 kbps
TCP (32)*	10	320 kbps

Table 4. The medical data rate of simulation samples

* Biomedical (vital) signals of emergency index (digital sphygmomanometer, digital thermometer, respiration, heart rate and ECG).

Besides, we also focus on the other variable of bandwidth in U-healthcare system of this QoS simulation. The parameters of other variable medical media are shown in Table 5.

Other variable	Down -link	Up-link	Explanation
Hospital using bandwidth	5M	1Mbps	Reserve bandwidth
Remote monitoring	—	384 kbps	Irregular traffic
Ultrasound, cardiology, radiology	—	256 KB (image size)	Irregular traffic
Magnetic resonance image	—	384 KB (image size)	Irregular traffic
Digital radiography	—	6 MB (image size)	Irregular traffic

Table 5. Other variable of U-healthcare QoS simulation

The scenario of simulation is assumed by us which is 10 patients using U-healthcare system simultaneously. The measurement scenario is shown in Fig. 8. The bandwidth of the uplink of FTTB is limited to 1Mbps, and the downlink bandwidth is limited to 5Mbps.

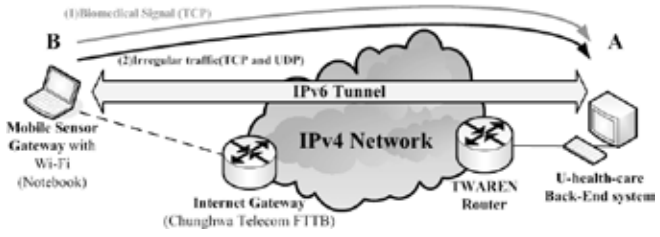

Figure 8. The measurement scenario of QoS

First, we test the biomedical data transmission without other variable medical media, then the transmission with *digital radiography* of 6M and *remote monitoring* streams of 384k bps at the same time, to obtain the packet loss of FTTB network caused by other variable medical media. The scenario of this simulation at point A is to obtain emergency data with QoS and without QoS (packet loss rate), whereas measurements at point B to obtain the characteristics of the irregular traffic injected to the uplink (delay).

4.2.1 QoS Evaluation Results (Delay)

The two simulation projects (IPv6 traffic class QoS and non-QoS) were initially conducted with delay simulation test. The results are shown in Fig. 9. We can clearly see that regardless under what data rates with irregular medical flow, IPv6 traffic class QoS was found to have a lower delay. And only in vital signals transmitted the delay is nearly non-differentiation (IPv6 traffic class QoS about higher than the non-QoS about 0.5ms). As a result of we set the simulation options for emergency packets to higher priority, so the medical data of low priority will undergo a large number of delays.

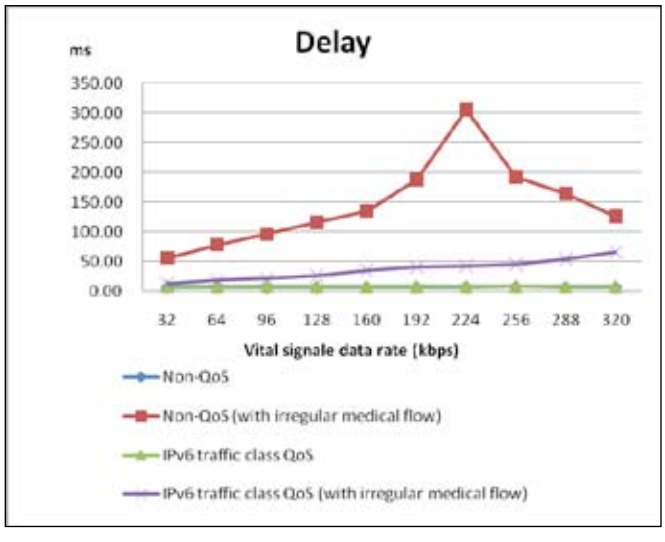

Figure 9. QoS evaluation results-delay

4.2.2 QoS Evaluation Results (Packet Loss Rate)

The results shown in Fig. 10 indicate that non-QoS with irregular medical flow had the highest packet loss rate because the network had two traffic (*digital radiography* of 6M and *remote monitoring* streams of 384k bps) transmitted at the same time. And it was caused the network had large delay, but it can be seen from Fig. 10, under the influence of the same factors that the IPv6 traffic class QoS can reduce the network delay effectively.

In addition, the two curves of IPv6 traffic class: QoS and non-QoS had shown significant drop in data rate after 224 kbps, but they had indeed shown a remarkable climb in the total packet

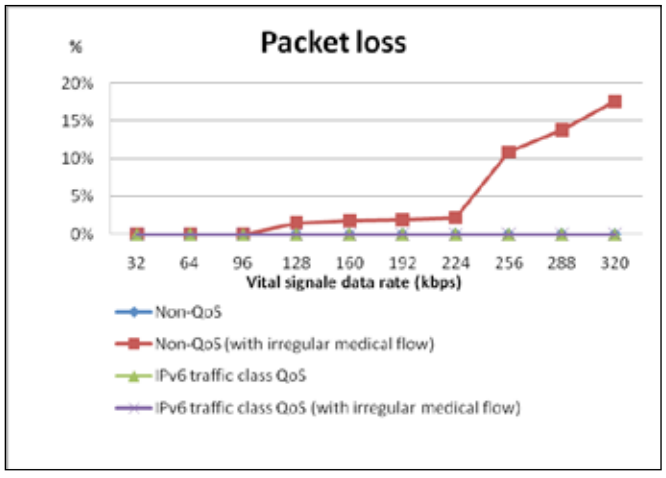

Figure 10. QoS evaluation results-packet loss rate

loss rate. We find that it was due to large amounts of irregular medical packets being discarded, so packet loss rate was increased. At this point, the packets on network had reduced, and the packets received from the server side had been reduced relatively, so delay was reduced.

5. Our Test System

5.1 U-healthcare Test System in Laboratory

We have established an IPv6 healthcare network in our laboratory, to experiment with the U-healthcare system: First, we install the U-healthcare sensors in this simulated healthcare environment, which includes a PDA-based mobile ECG measurement system, In-door positioning system, acquisition of physiology signal and RFID application. Each sensor will be connected to the network through an IPv6 sensor node. The sensor node will be a PC or notebook in a nursing car.

Through the RFID identification, users can login to the backend data base to inquire about family health status. In the care center, nurses can measure, record and observe the health and medical information of the patient with greater convenience

The care information and networks are managed by the care service center. Internal network uses the IPv4/IPv6 dual stack router to handle routing of external network. The LAN network is cut into two sub networks: (1) servers and IPv6/IPv4 website, and (2) care service sensing device in the demonstration site. The server sites provide services, such as: IPv6 web, DNS, data base and SIP.

Finally WAN is connected by the IPv4/IPv6 dual stack router through the “TANET” external network to provide internet services. The IPv6 connection is through a tunnel to *academia sinica* server. This connects to hospitals and care centers to provide remote medical analysis of the hospitals in China Medical University Hospital (CMUH) and health care centers in China Medical University Beigang Hospital (CMUBH) to do the test. The network structure is shown in Fig. 11.

5.2 Test in Hospital

We choose China Medical University, Beigang Hospital Taiwan, to test our U-healthcare system in a clinical environment. The test environment was on one floor of the hospital: ward 16, with eighty patients and five nursing staff. The test was conducted using a Bluetooth sphygmomanometer on the nursing car. The procedures of U-healthcare network practice in the hospital with security and QoS methods are shown in Figure 12 and as follows.

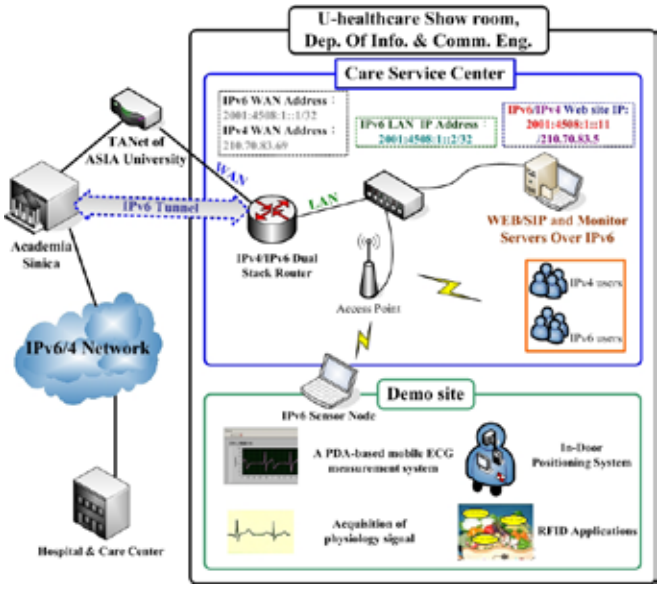

Figure 11. Our IPv6 healthcare network structure

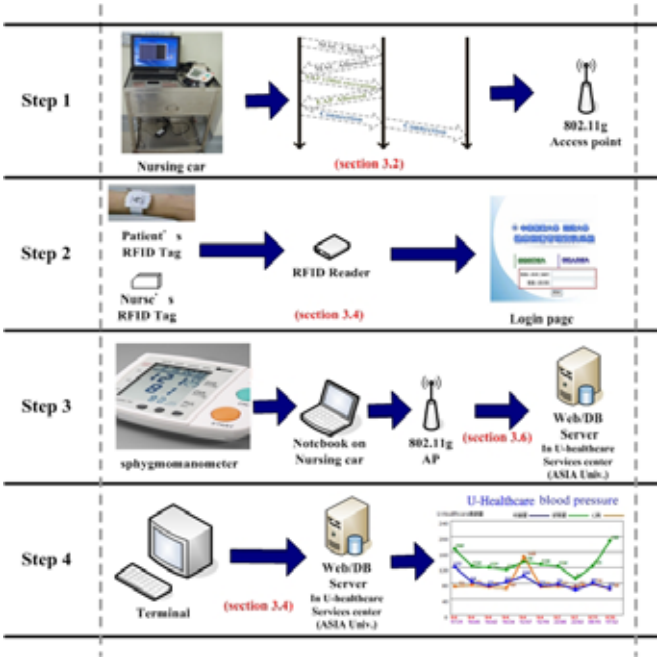

Figure 12. Procedure of U-healthcare network test in the hospital with security and QoS methods

First, a notebook was connected to the WLAN through a physical layer protection (section 3.2). The nurse is required to confirm patient identity by RFID (section 3.4), prior to beginning the measurement. And the measurement data is transmitted to the back-end database system storage. When the history of blood pressure monitoring and query value, it must be the security infrastructure (section 3.4) in order to login the health-care information website.

Finally, the WAN is connected to the hospital emergency room through (section 3.6) to provide QoS and backup functions.

6. Conclusions

When the closed-wire medical sensor system evolves to the ubiquitous healthcare sensor system, it will face the problems inherent in wireless networks, viz; issues of security, quality of service, and network issues. In this paper, we study the problems of a ubiquitous network with the QoS and security, and then evaluate and practice this ubiquitous network in the hospital. This will contribute to the future development of a U-healthcare system, and provide a reference for both security and QoS networks. At the same time, through the framework of our ubiquitous network experiments, the integration of the city's hospitals with urban medical care can provide an improvement to healthcare resources in countryside. Finally, in anticipation of the future of the 'All IP' age, the U-healthcare system with security and QoS will be commonly used in daily life, to the enhancement everyone's standard of living.

Acknowledgment

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grant NSC99-2221-E-030-022 and supported in part by China Medical University under the grant 9600000027. Our gratitude also goes to Dr. Timothy Williams, Asia University.

Reference

[1] Lin, Chung-Chih., Lee, Ren-Guey., Hsiao, Chun-Chieh (2008). A pervasive health monitoring service system based on ubiquitous network technology, *International journal of medical informatics*, 77 (7) 461–469.

[2] Pallikonda Rajasekaran, M. Radhakrishnan, S., Subbaraj, P. (2009). Elderly patient monitoring system using a wireless sensor network, *Telemedicine and e-Health*, 15 (1) 73-79.

[3] Kumar, Sunil., Kambhatla, Kashyap., Hu, Fei., Lifson, Mark., Xiao, Yang (2008). Ubiquitous computing for remote cardiac patient monitoring: a survey, *International Journal of Telemedicine and Applications*, 4 (3).

[4] Oh, Se-Jin., Lee, Chae-Woo (2008). U-healthcare sensor grid gateway for connecting wireless sensor network and grid network, *10th International Conference Advanced Communication Technology, (ICACT 2008)*, v. 1, p. 827 - 831, Gangwon-Do.

[5] Jovanov, Emil (2006). Wireless technology and system integration in body area networks for m-health applications, *In: Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, p. 7158-7160, 17-18 Jan.

[6] Pindter Medina, J., Gonzalez Villarruel. J E., Tovar Corona. B, (2009). Proposal for an m-Health System, *2009 Electronics, Robotics and Automotive Mechanics Conference*, p. 55-59.

[7] Lemma, Fikreyohannes., Denko, Mieso K., Tan, Joseph K. (2008). Envisioning a national e-Medicine network Architecture in a developing Country: A Case Study, *International Journal of Healthcare Information Systems and Informatics*, 3 (1) 44-62.

[8] Chigan, Chunxiao., Oberoi, Vikram (2007). QoS Provisioning in Sensor Enabled Telemedicine Networks, *International Journal of Healthcare Information Systems and Informatics*, 2 (3).

[9] Chigan, Chunxiao., Oberoi, Vikram (2006). Providing QoS in Ubiquitous Telemedicine Networks, *In*: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)

[10] Martinez, Ignacio., Garcia, Jose., Viruete, Eduardo A.(2008). Resources Variability in m-Health Services:

An Adaptive Method for QoS Control, *IEEE CCNC 2008 proceeding*, p.829-833.

[11] Philip, N., Robert. S. H. (2007). Medical Quality of Service for Wireless Ultrasound Streaming in Robotic Tele-Ultrasonography System, *In: Proceedings of the 2007 IEEE International Conference on Networking*, Sensing and Control, p. 245-250, London, UK, 15-17 April.

[12] Perkins, C., Johnson, D (2000). Route optimization in mobile IP, *Internet Draft, Internet Engineering Task Force*.

[13] Perkins, C., Johnson, D. (1998). Route optimization for Mobile IP, *Cluster Computing*, 1 (2) 161–176.

[14] Zagar, Drago, Grgic, Kresimir., Rimac-Drlje, Snjezana (2007). Security aspects in IPv6 networks – implementation and testing, *Computers and Electrical Engineering*, 33 (5-6).

[15] Dagtas, S., Pekhteryev, G. S¸ahinoglu, Z., Cam, H., Challa, N. (2008). Real-time and secure wireless health monitoring, *International Journal of Telemedicine and Applications*, v. 2008, 4 (1).

[16] Stanford, V. (2002). Pervasive health care applications face tough security challenges, *IEEE Pervasive Computing*, 1 (2) 8-12.