Integrated Hospital Information System with IPv6 for Ubiquitous Healthcare Environment

곽동엽, 문강남, 이정훈, 토니 사하마, 김정태*
퀸즈랜드공과대학교, 목원대학교*

Integrated Hospital Information System with IPv6 for Ubiquitous Healthcare Environment

DongYeup Kwock, KangNam Moon, JeongHoon Lee, Tony sahama. Jung-Tae Kim*

Queensland University of Technology, Mokwon University*
E-mail : *dong.kwock@connect.qut.edu.au*,

Abstract

IPv6 and Ubiquitous Healthcare Environment (UHE) has become a main stream of the next generation technologies. IPv6 is designed in many ways with enhanced features such as a routing, mobility, scalability, QOS and security as a replacement of IPv4. Also, UHE is developed to provide patients with convenience and efficient healthcare services using the remote home healthcare system. However, IPv4 currently used as an Internet protocol does not have enough capability to fully support UHE. It may result in a restricted implementation of UHE. As a result, research on IPv6 implementations in UHE is increasingly becoming an issue within the healthcare industry. IPv6 has enhanced features to implement the remote healthcare system such as Neighbour Discovery process and address auto-configuration. In this paper, a basic of IPv6 and UHE will be firstly introduced and secondly, benefits brought by IPv6 in UHE will be discussed. In addition, security issues in IPv6 will be analysed to conclude this paper.

Key Words
IPv6, UHE, Remote Healthcare, MIPv6, Security

Ⅰ. Introduction

With a wide spread of the Internet, IPv4 addresses are being rapidly exhausted [1]. Also, an introduction of ubiquitous environments may accelerate the exhaustion problem due to the fact that a huge number of IP addresses will be used for Ubiquitous Sensor Network (USN) and various wireless devices. To resolve the problem, IPv6 has been invented as a replacement of IPv4. One of the major advantages features about IPv6 is that it provides an extended address capacity which is four times larger than what is permitted with IPv4.

In the same way, healthcare services have also evolved to the Ubiquitous Healthcare Environment (UHE). In UHE, a use of various wireless technologies and devices has been increased which contributes to consume more IP addresses. In the near future, hospitals will be faced with a problem concerning their network system whether it should be changed to the IPv6 network system due to the limitation of IPv4. Nevertheless, the hospitals have no idea how IPv6 will contribute to their healthcare service. For these reasons, this report will further discuss the features of IPv6, beginning with an introduction of the UHE and

secondly IPv6's benefits for UHE will be analysed with its possible security issues.

II. Background of IPv6 and UHE

A stream of IT technology is moving to the next generation. IPv6 and UHE are a main stream of the next generation technologies. In this section basic features of IPv6 and UHE will be introduced.

2.1 Features of IPv6

As defined in RFC2460 [2] the datagram in IPv6 is designed to be simpler than that of IPv4. The main reason for the design is to boost the processing performance, because a simpler header format makes the routing process faster. To make it simple, the IPv6 utilizes an additional header space which is called the extension header. While the essential fields are placed in the IPv6 datagram header, the extension header contains all additional information such as special routing information and fragmentation options.

One of the main reasons of the IPv6 development is to create enough IP address space for future growth. As defined in RFC3513 [3], an IPv6 address has 128 bits length, four times bigger than a 32 bit IPv4 address. This allows the creation of 2^{128} addresses, whereas 2^{32} addresses are the maximum number of addresses possible in IPv4. IPv6 has a different format compared to IPv4 and related address presentation rules are "Colon separated address", "Leading zero compression", and "Address prefix". Unlike "dot-decimal format" of IPv4, IPv6 separates digits with colons.

Colon separated IPv6 format:
2002:abcd:0123:0a45:0000:0000:abcd:b111

Also, Neighbour discovery protocol in IPv6 is used to announce the existence of each node in an IPv6 network and to discover other nodes' in existence. As defined in RFC2461 [4], the neighbour discovery is a compulsory process for any node which has IPv6 installed. The main features of the neighbour discovery protocol are as follows;

- *Router discovery, Prefix and Parameter discovery*
- *Address auto configuration and resolution*
- *Next-hop determination*
- *Neighbour unreachability detection*
- *Duplicate Address Detection*
- *Redirect*

The Neighbour Discovery Protocol employs four patterns of ICMPv6 packets to implement the features defined above. These four patterns are Router Solicitation, Router Advertisement, Neighbour Solicitation and Neighbour Advertisement.

Router Solicitation (RS): *A Host sends a RS message to a router in order to get a Router Advertisement message. A Host forwards the Router Solicitation message as soon as an interface on the host is turned on. Router Solicitation uses 'ff02: 2' to be sent to all routers on a link-local site.*

Router Advertisement (RA): *A RA message is sent by a router as a response of a Router Solicitation message and routers also forward Router Advertisements periodically to advertise their existence. If multicast is available on a link, routers periodically send Router Advertisement messages using all-nodes multicast (ff02::1). Hosts which receive Router Advertisement messages renew their default router list and may gain prefix information and hot-limit which can be used for auto configuration.*

Neighbour Solicitation (NS): *A NS message is employed to perform three things which are address resolution, neighbour unreachability detection and Duplicate Address Detection. For example a node asks a link-layer address for a destination.*

Neighbour Advertisement (NA): *Generally NA responds to 3 types of Neighbour Solicitation and is also generated without Neighbour Solicitation in order to propagate new information.*

2.2 UHE Features and Issues

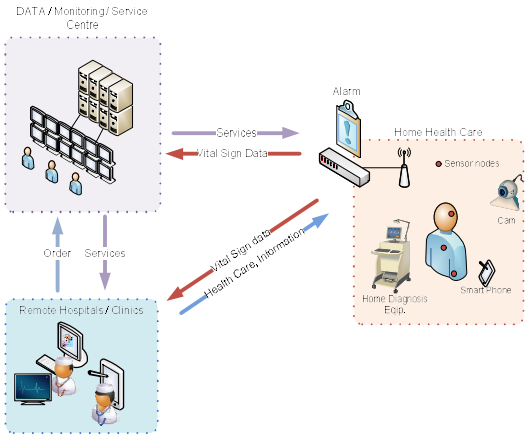

Figure 1. Example of Remote Healthcare Service

The main point of UHE is a remote healthcare service called Telehealth. It means that patients can take a medical treatment at home using their own devices. As shown in figure1, patients and remote health service centers are firstly connected through dedicated communication lines through the Internet. Next, doctors are able to diagnose their patients using a video call and remote medical equipments. There is no apparent difference from face-to-face diagnosis because the remote medical examination implements visual inspection, history taking except a palpation or percussion. Also, doctors can prescribe a prescription based on the medical test results. If the patients need to take drugs, the prescription will be sent to their homes through the communication line on the Internet. With the development of Telehealth and the spread of the Internet, the use of remote home healthcare services has accelerated. Also, home diagnostic equipments for simple measurements such as blood sugar and cholesterol meters are readily available for purchase and are becoming common in households. When we look inside a clinical environment, it is common that a lot of chronic patients visit just for a medical consultation or prescriptions. Therefore, it is not deniable that Telehealth is a practical mechanism for both hospital staffs and patients. Furthermore, Telehealth has recently evolved another step further. With mobile devices and USN, Telehealth services are extended further. Firstly, sensors are attached on the patients' body monitoring their vital signals in real time. The results are also regularly updated to the database in a hospital which will be used for an analysis of the patient's condition. Secondly, mobile devices such as a smart phone remove space constraints so that healthcare services are only provided in particular places such as hospital and house. With mobile devices, patients are available to take healthcare services anywhere as long as patients have the access to the internet. Mobile healthcare systems can be restricted in several services, but it will be varied as hardware and software on mobile device are developed. However, there are some difficulties and problems to implement Telehealth under the IPv4 network because of the lack of IP addresses and scalability and efficiency, but those issues will be resolved with the use of IPv6.

Ⅲ. Benefits of IPv6 for UHE and Security Concerns

IPv6 and UHE will co-operate to lead future hospital information systems with their enhanced advantages. Benefits of IPv6 for UHE and its security concern will be discussed throughout this section.

3.1 Benefits of IPv6 for UHE

The use of IPv6 in UHE may bring benefits such as enhanced mobility, scalability and security. In this section, those major benefits of IPv6 in UHE will be described as well as how they will work in UHE.

Enhanced mobility: In the Ubiquitous Healthcare Environment, it is an issue how mobile patients are efficiently supported without the complicated process to re-connect with the hospital network system whenever they move to new places. Currently, Mobile IPv4 (MIPv4) is utilized for mobile users in the IP network. In the healthcare service, Mobile IP is always using Home Address (HA) to communicate with a hospital even if patients are far away from their home. When patients stay at home, their Mobile Nodes (MN) just use HA to communicate with the Hospital, but one more address is required when patients are in a foreign network. In the foreign network, Care of Address (COA) is assigned to the patient by a foreign agent and utilized between home and the foreign network. The patient firstly needs to bind COA with HA. After the binding process, the home agent enables to intercept all packets destined to HA, encapsulates packets with COA and tunnels packets to the patient at the foreign network. However there is a problem regarding efficiency such as triangular routing problems which means that packets always have to go through the home network to reach patients in the foreign network.

In IPv6, Mobile IPv6 (MIPv6) [5] is also designed in the same way as MIPv4, and MIPv6 has enhanced features to make up for the weak points of MIPv4. Table1 shows comparisons between MIPv4 and IPv6.

Table 1. Comparison between MIPv4 and MIPv6

Mobile IPv4	Mobile IPv6
• Add-on feature • Foreign Agent	• Integrated into base IPv6 protocol

required • Triangular Routing Problem	• Foreign agent not required (ND & Add auto configuration) • Route Optimization

In IPv4, Mobile IP is one of add-on features that the network admin should configure additionally, but MIPv6 is integrated into the base IPv6 protocol and implemented automatically as needed. When patients move to the new network, their mobile nodes start the router discovery process. Firstly, mobile nodes broadcast the RS to get the RA from a router in the new network. Once patients receive the RA, a new COA is automatically generated using auto configuration features. This process eliminates the foreign agent used in MIPv4 which is to provide the patient's mobile nodes with its CoA and tunnel packets.

Furthermore, MIPv6 enables the direct communication between the mobile patient and the hospital. As shown in figure 1, it is called the route optimization with which the patient can send data to the hospital without their home agent after the binding update between mobile patients and the hospital. Therefore, the data transmission between the patient and the hospital can be faster due to no intermediate node. In addition, the connection to hospitals via home agents remain as an alternative path in case the direct connection is failed. It means the route optimization also guarantees availability for the mobile healthcare service.

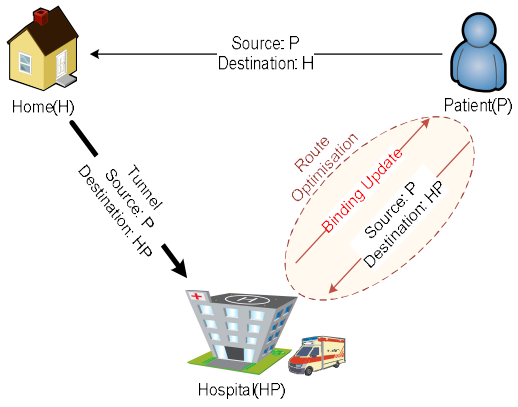

Figure 2. Route Optimization of MIPv6

Body Sensor Network Support: Body sensor networks will be attached on a patient's body for monitoring patient's conditions in UHE wherever they move. Currently, ZigBee non-IP protocol is generally employed to implement sensor networks as a low-power wireless technology. However, it is an obvious fact that implementation of IP protocol on the sensor network may efficiently assist the sensor network management. In fact, IPv4 do not have enough capability for sensor network compared to ZigBee protocol, while IPv6 has enhanced features to support sensor networks such as a large address capacity, Neighbour Discovery protocol and the address auto-configuration. Currently, researches about IPv6 for sensor networks have been conducted by a working group IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) [6]. Sensor nodes with low power, minimised memory and process to support for IPv6 are being developed and expected as a replacement of ZigBee.

Also, Network Mobility (NEMO) protocol [7] which is designed based on IPv6 can be implemented to support the sensor network. Using MIPv6 for each sensor node is not efficient due to the restricted power supply and computing capability of sensor nodes. To resolve this problem, NEMO employs Mobile Router (MR) to use as a gateway for sensor nodes. With MR, sensor nodes can maintain their network status wherever they move because MR also moves with the sensor nodes. Therefore, MR only needs to configure itself to adjust into a new network.

3.2 Security Concern

In UHE, security aspects should be measured before the IPv6 implementation because small security vulnerabilities may result in serious incidents. In IPv6, several attack methods as in IPv4 can be made using Neighbour Discovery process of IPv6. [8]

Man-in-the-middle: This attack method is based on address resolution protocols in the ND process. Neighbour solicitation can be intercepted by the attacker. The attacker then responds to the Neighbour Solicitation with a Neighbour Advertisement which has a manipulated MAC address. Also, the attacker is able to act as a router on the LAN. Usually a router periodically sends a Router Advertisement message to all nodes in a link-local site, and all nodes which receive Router Advertisement set their routing table and network prefix based on the Router Advertisement. This mechanism allows the

attacker to disturb the routings of all the link-local nodes.

Moreover one more attack can be made using the Duplicate Address Detection function. As a new host it is connected to a LAN which sends a Neighbour Solicitation message using the multicast (FF02::1) to check if this link-local IPv6 address is already existing or not. The host uses this link-local address only if no Neighbour Advertisement is received during a specific period of time. Using this mechanism, the attacker monitors the network for Duplicate Address Detection messages, and when detected, it sends a Neighbour Advertisement back to interrupt the creation of new link-local addresses. Because the host receives a Neighbour Advertisement, with the IP Address it would like to use, this IP gets marked while in use and a new IP address will be generated and a new Duplicate Address Detection message will be sent. This happens until specific amounts of attempts have happened, then the system will stop trying to get an IP address and will not connect to the network.

Denial of Service: This attack uses the victims IP address as the source address of the ICMPv6 Echo request and uses the link-local-multicast (ff02::1) as the destination. Doing this, every device on the local link will respond to the Echo request and will send the Echo reply to the victim. Using this method, a huge amount of packets can be generated in a short amount of time. The attack grows larger as more devices are on the local link.

Ⅳ. Discussion and Conclusion

As mentioned through this paper, IPv6 has a great mobility feature so that a restriction of mobile healthcare services is expected to minimise. Also, it will eventually result in a wide spread of UHE in the healthcare industry, and patients will be able to receive healthcare services wherever they are. However, the migration to IPv6 should be conducted step by step and the compatibility and the security issues should be measured properly before the use of IPv6. In fact, IPv6 also has enhanced security features than IPv4. Therefore, those attacks mentioned above can be managed easily as long as a network admin recognises those security issues of IPv6. In the future, a practical test of integration IPv6 with UHE should be conducted. Through the test, possible errors and unexpected issues can be resolved and found.

References

[1] Huston, G. (2009, MAY 11). IPv4 Address Report. Retrieved SEP 28, 2009, from http://www.potaroo.net/tools/ipv4/index.html

[2] Hinden, R., and Deering, S. (1998, DEC). RFC2460 - Internet Protocol, Version 6 (IPv6) Specification. Retrieved SEP 23, 2009, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc2460

[3] Hinden, R., and Deering, S. (2003, April). RFC3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture. Retrieved SEP 22, 2009, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc3513

[4] Narten, T., Nordmark, E., and Simpson, W. (1998, DEC). RFC2461 - Neighbor Discovery for IP Version 6 (IPv6). Retrieved OCT 1, 2009, from The Internet Engineering Task Force: http://www.ietf.org/rfc/rfc2461.txt

[5] Johnson, D., Perkins, C., and Arkko, J. (2004, JUN). RFC3775 - Mobility Support in IPv6. Retrieved OCT 03, 2009, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc3775

[6] Kim, E., and Kim, Y. (2007). 6LoWPAN Based IP-USN Standardization. Korea: ETRI.

[7] Devarapalli, V., Wakikawa, R., Petrescu, A., and Thubert, P. (2005, JAN). RFC3963 - Network Mobility (NEMO) Basic Support Protocol. Retrieved OCT 02, 2009, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc3963

[8] Hauser, v. (2006, October 24). THC-IPV6 - attacking the IPV6 protocol suite. Retrieved OCT 03, 2009, from The Hacker's Choice: http://freeworld.thc.org/thc-ipv6/