International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:10, 2007

Investigating the Possible use of Session Initiation Protocol for Extending Mobility Service to the Biomedical Engineers

Anwar Sadat

***Abstract*—**Today, the Internet based communication has widen the opportunity of event monitoring system in the medical field. There is always a need of analyzing and designing secure and reliable mobile communication between the hospital and biomedical engineers mobile units. This study has been carried out to find possible solution using SIP-based event notification for alerting the technical staff about the Biomedical Device (BMD) status and Patients treatment session. The Session Initiation Protocol (SIP) can be used to create a medical event notification system. SIP can work on a variety of devices. Its adoption as the protocol of choice for third generation wireless networks allows for a robust and scalable environment. One of the advantages of SIP is that it supports personal mobility through the separation of user addressing and device addressing. The solution for Telemed alert notification system is based on SIP - Specific Event Notification. The aim of this project is to extend mobility service to the hospital technicians who are using Telemedicine system.

***Keywords*—**Biomedical, Mobility Service, Notify, Proxy Server, SIP, Subscribe, Telemedicine.

I. Introduction

A telemedicine system is a deployable IT solution that allows a health care organization to monitor and manage remote medical devices located within a healthcare environment or placed in patient homes. The BMD is mainly support systems for breathing, such as ventilators, Bi-level apparatuses, CPAPes, equipment for oxygen therapy such as oxygen concentrators and surveillance equipment such as pulsoximeters and capnographs. The equipments used by the patients are for making it possible to sleep and to avoid dangerous interruptions in breathing that could otherwise lead to poor quality of life and a great risk for such diseases as cerebral vessel disease, high blood pressure and heart attacks.

The use of biomedical equipment in the home environment has increased rapidly [1] during the last decade. The complexity of such equipment is also increasing. The increase depends both on new treatment methods and an increasing number of patients that are treated in their homes [2]. To maintain a secure and safe home healthcare, the equipment is frequently maintained by some technical service unit, normally the hospital biomedical engineering department.

The general architecture of the platform for connecting BMDs in patient homes to the hospital could be defined and implemented as shown in the diagram below:

Anwar Sadat is with the School of Science and Technology Bangladesh Open University, Board Bazar, Gazipur 1705, Bangladesh.

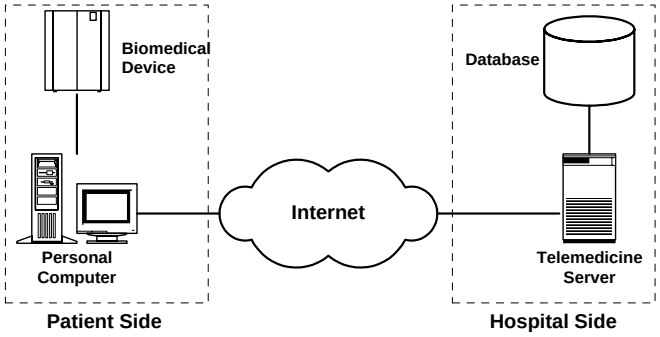

Fig. 1 General architecture of the platform

A BMD is connected through the serial port to a standard PC in the patient's home which in turn communicates with the server located at the Hospital by using an Internet connection and sends the relevant information to the repository in the Hospital. All server-to-server and client-to-server communication is managed through the SSL protocol for encryption and authentication.

Problem Description

The use of biomedical device (BMD) in the home environment is increasing rapidly. The complexity of such equipment is also increasing. The increase depends both on new treatment methods and an increasing number of patients that are treated in their homes [2]. Using biomedical devices in the patient home environment is an effective mechanism in maintaining patient quality of life and is more effective in the utilization of patient care resources and funding. This increase in efficiency is driving the increase in the use of biomedical devices into the patient home environment. As the number of devices increases, different kinds of problems arise. To maintain a secure and safe home healthcare, the equipment is frequently maintained by some technical service unit, normally the hospital biomedical engineering department. Let us look at a real-life scenario to get a distinct depiction of the shortages we experience with this approach.

Patients, who are using a BMD device at home, sometimes face problems operating the device properly or fall in difficulties when the BMD malfunctions. When these happen, they call the biomedical engineers at Hospital. Technical staffs then try to solve the problem over phone. Otherwise they need to go to the patients home immediately to find out the actual problem. Sometimes, the failure occurred due to the lack of

knowledge of the patient, but in some cases it depended on the malfunctioning of the device.

To support this home healthcare service, a technical platform has been designed and implemented which will facilitate remote monitoring of the BMD devices. In this system, Patient part of the application will send the BMD data to the server located at the hospital and the Hospital part of the application will be used by the engineers for monitoring the BMD status based on the transmitted data. When the new technical application system will start working, engineers will need to monitor the status of the BMD continuously. As they have to stick to the system, their valuable time will be wasted. Suppose, for the time being, the engineers become busy with other devices or they need to go far from the technical application. At that time, Hospital part of the application displayed a message that one BMD device has gone out of order. But as the technicians are not constantly monitoring the system, this event remains unnoticed and unhandled for a long time. This situation may result in some unexpected damage to the patient life, which will ultimately degrade the home health care system.

From the scenario presented above, we can elicit some drawbacks. As discussed earlier, while the technical system will start working, biomedical engineers will need to be physically in touch with the application system all the time to monitor the BMD status. Stick to a location where the technical application is installed doesn't allow mobility to the technician. Even if a technician visits a patient's home to solve the problem of the device, he has to come back to the MTA to get new service call, because the application system is installed in a fixed place. This will be wastage of technician's valuable time to travel around and also inefficient use of his expertise. To be more efficient in the use of time and expertise, engineers need certain degree of mobility while they are at work. By adding the mobility feature to the system, engineers will be always updated with the present status of the devices located at patients' home without being physically in touch with the application system at hospital. This will also give them an opportunity to utilize modern communication technology in their daily working routines. Realizing the fact that the engineers need to be in touch with the system all the time, it is evident that we need an efficient solution, which will add mobility feature to the application. Then we should conclusions with the following questions:

- What will be possible technology solution to provide mobility?
- How much secure the proposed system will be?
- Would the system added with new technology feature be easy to operate?
- How much feasible the system will be in terms of cost and healthcare service?

The scope of this paper is limited to carry out detail analysis and design of facilitating secure and reliable mobile communication between the hospital and engineers mobile units using SIP-based event notification for alerting the technical staff about the BMD status and patients treatment session. Therefore, the goal is to facilitate secure and reliable mobile communication between the application system in hospital and biomedical engineers mobile units using SIP-based event notification for alerting the technical staff about the BMD status and Patients treatment session

II. Overview of Related Works

A. A SIP-based Medical Event Monitoring System [3]

Event notification systems are being used increasingly in many different disciplines. There are various uses for event notification systems in medicine, such as in patient monitoring systems both within a hospital and remotely, doctor-to-doctor communication, monitoring drug interactions when a doctor prescribes different medications, reminders of appointments or medications to be taken, etc. Recently, the Internet is being used in a larger scale to establish communication between doctors and patients.

Creation of a medical event monitoring system using the Session Initiation Protocol (SIP), a signaling protocol used for establishing, modifying and terminating sessions with one or more participants on the Internet has been proposed. SIP has gained momentum in IP telephony as the protocol of choice and has also been accepted as the underlying signaling protocol for third generation wireless networks (3GPP). Additionally, SIP supports SUBSCRIBE and NOTIFY methods as used in event notification systems. Therefore authors have considered SIP to be the suitable choice for our medical event notification framework.

The paper discussed how SIP is used in medical event monitoring systems. Also authors have proposed a SIP medical event monitoring system which can use Medical Logic Modules, such as the Arden Syntax or XML documents in order to filter specific event notifications. Finally, authors have presented an integrated architecture of various devices and protocols that can be part of the SIP event notification system.

B. SIP-based Emergency Notification System [4]

The Emergency Broadcast System (EBS) was developed in 1963 to notify the public of emergency situations. In December 1995, the Federal Communications Commission (FCC) changed the EBS to the Emergency Alert System (EAS). This change signified a different way state and local governments provide the emergency notification and instruction to the public. The EAS uses digital technology that functions similarly to computers. It automates the notification process and specifies the requirements of when and how to provide the emergency instruction to the public. Thus, the state and local governments can inform the public through radio, television and cable stations without the need for the broadcast industry to be present. The EAS can also transmit this information to a specific location in an emergency situation, as long as there have been predetermined arrangements of the communication links.

The EAS is controlled by the government and used mostly for wide area emergency notification. However, there are emergency notification networks and products that offer

emergency alerting in a localized area. In particular, Reverse 911 offers emergency notification service to local officials or companies who can subscribe to the network and receive any emergency notifications that occur in the nearby vicinity. The subscription includes preferences regarding the geographical location of the notification, the types of emergency alerts, and the alert method, such as sounding off an alarm or siren, flashing lights, an instant message or telephone calls. The subscriber will provide a list of local phone numbers to the notification network, which will then monitor that location of any emergency situation it had registered for and notify it in case of an emergency.

This paper described how the Session Initiation Protocol can be used to implement an emergency notification system. This system offers advantages such as portability, lower resource consumption, and an additional means of reaching people in case of an emergency. Although SIP is an Internet-based system, it would not interfere with the current EBS system, but instead complement it. As the system exists today, emergency broadcasts are done via radio and television. This could be integrated with the SIP-based emergency system to provide emergency notifications via the Internet as well.

III. Requirements Analysis

A. User Requirements

Biomedical engineers, who will be the user of the system, need a system to get rid of the immobile working condition. The immediate impact is to efficiently deploy their services to where they are mostly needed. Present problems were analyzed to realize the user and system requirements. Several ideas and expectations were taken into account in defining the system model. As a result of the elicitation process, the functional requirements on the system were defined. Improvements were considered as the system evolved.

B. Functional Requirements

Whenever Telemedicine application system receives BMD data uploaded by the patient, the system compares these data with the standard and prescribed data stored in the system for that particular device. If the received data doesn't show the correct or recommended value, then the application system will generate an alert message. Alert message will contain information like, BMD serial number, type of the device, message arrival time, BMD location, patient name and address, etc. This notification need to be transported to the technician wherever he is staying. It is likely that traditional modes of communication will be augmented by Internet telephones and applications in the near future. Thus, we need to have emergency notification systems established on the Internet.

IV. Selection of Technology

A. Why SIP?

SIP has been standardized by the Internet Engineering Task Force (IETF) as a fundamental piece of the Internet architecture. Simplicity of Session Initiation Protocol (SIP) and the fact that it is Internet standards based, gives it clear advantages over older protocols. SIP is very useful for finding and "connecting to people," regardless of where they happen to be or what they are doing. The SIP-event notification mechanism allows a SIP entity to request notification from remote nodes indicating that certain standardized events have occurred. Examples of such of events are changes in presence states, changes in registration states, changes in Subscription authorization policies and other events that are caused by information changes in e.g. Application Servers.

One of the chief strengths of SIP is its ability to interact with other communications protocols, and to tie together multiple features into more advanced services. SIP's heritage of text-based, header-and-body protocols, such as HTTP, SMTP, and RTSP, is a key to its rapid adoption. The benefit of SIP is that it is a core technology with uses in many applications beyond VOIP including Presence & IM, Rich Calls, Push To Talk, Interactive Gaming, Push, presence & location-based services, etc. Also, it can be used in combination with other technologies such as HTTP/WAP, SMS/MMS to create enhanced services. Compared [1] to existing systems, elements of the SIP technology and business value proposition include but are not limited to

- Presence (i.e. a group of individuals can share information)
- Combinational services (to combination of services, such as directory information, Web browsing, positioning, and presence)
- Access independence (SIP offers seamless service capabilities between fixed and mobile networks)
- New charging models (able to define new charging models based on actual media usage)
- Quality of service (SIP-based products sit on top of the IP network and take advantage of the capabilities of the underlying network to provide QoS)
- Security (SIP can encrypt and authenticate signaling messages; RTP supports the encryption of media)

B. Other solutions

It is obvious to ask why not other protocol should serve the need of the problem. The following sections describe the arguments applied in rejecting possible alternatives.

HTTP

The Hypertext Transfer Protocol (HTTP) is the basis for most Web communication. A Web server, with the services/applications offers Web pages. HTTP does not provide good support for mobility and notifications. Additionally, current HTTP must run over TCP, and a TCP stack is larger and more complex than a UDP stack. In addition, HTTP is inherently a client/server protocol, which does not map well to asynchronous notification scenarios.

SMTP

The Simple Mail Transport Protocol (SMTP) seems, on first inspection, a likely candidate for asynchronous communication since it supports an application-level addressing scheme, carries a flexible payload, and supports mobility, as exploited in e-mail forwarding. However, SMTP

does not support events and media-based sessions, and it can exhibit extremely high latency.

SNMP

The Simple Network Management Protocol (SNMP) is already popular for Internet-based network management. The client device is mobile and need an application layer name but SNMP only supports network-layer addressing. Furthermore, SNMP does not support multimedia sessions.

V. Proposed SIP based Solution

By adding the mobility feature to the system, the biomedical engineers will be always updated with the present status of the devices located at patient's home without being physically in touch with the application system at hospital. Thus they will be able to utilize their time and expertise more efficiently to help the patient. This will also give them an opportunity to utilize modern communication technology in their daily working routines.

Recently, the Internet is being used in a larger scale to establish communication between doctors and patients. The Session Initiation Protocol (SIP) can be used to implement a notification system. This system offers advantages such as portability, lower resource consumption, and an additional means of reaching people in case of an emergency. SIP can provide a quick and efficient way of informing the people about an emergency situation. Thus, we can have emergency notification systems established on the Internet. SIP, which is an application-layer signalling protocol, has been used for maintaining sessions of Internet multimedia conferences, Internet telephony calls, instant messaging and event notification. SIP can work on a variety of devices; its adoption as the protocol of choice for next generation wireless networks allows for a robust and scalable environment that can easily extend across institutions.

SIP is the new standard for establishing multiparty, multimedia communication in IP-based networks. The telemedicine application server can send messages to the SIP endpoints. This could be done based on a SIP Subscribe-Notification message exchange containing the service information. In addition, the end point should also be able to send acknowledgement and other necessary information to the server. This information will be delivered using SIP based messages. Information in these messages may include e.g. text message, pictures, http, url, etc. SIP endpoints are used to make and receive calls. They can either be PDA, IP phones, software running on a PC, or a combination of an analog telephone adapter with a basic black phone. SIP servers contained with the call control system provide location, proxy, redirection, and registration services.

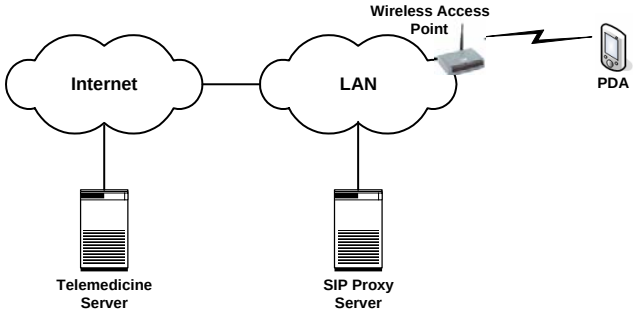

Fig. 2 SIP-based notification system Model

An example of a SIP based notification system model in illustrated in Fig. 2. Here, a technician will be able to receive alert message from Telemedicine platform. According to this concept, the current location of a user is hidden behind a permanent user identity or uniform resource locator (URL). A network-based SIP server binds the user's mobile identity to the permanent URL much in the same way a home agent functions in a mobile IP network. The two principal mechanisms in SIP that support this are redirection and proxying.

A. Underlying Technology Overview

The main technologies used in this application are:

- Session Initiation Protocol
- Session Description Protocol
- User Authentication

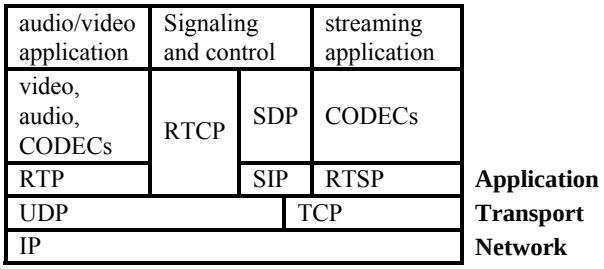

Fig. 3 Relationship of various protocols

B. Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is a standard for initiating, modifying and terminating communication sessions; it lies within the application layer of the OSI reference model, as shown in Fig. 3, and is independent of the underlying layers. It is based on HTTP/1.1, and features few message interactions per session, as well as simple analysis and debugging due to its text-based encoding.

Each SIP user has a unique address with the prefix "sip:" and then <entity>@<location>. For example: sip:bob@xyz.pda.net Each such address constitutes a SIP Uniform Resource Identifier (URI).

The Session Initiation Protocol (SIP) [5] meets the requirements for application layer messages communication. SIP allows flexible payload and provides end-to-end security. These features make it an attractive base for a solution. Like other signaling protocols, there are a few types of requests and many types of responses. A SIP based system can be as simple as two devices sharing the same Ethernet cable or as distributed system of servers and endpoints spanning several geographical locations. SIP routes messages using a hop-by-hop routing algorithm based on rewriting message headers.

C. Session Description Protocol (SDP)

The Session Description Protocol (SDP) [6] is a separate IETF standard used by SIP to describe the session. It is, like SIP, text-based, consists of a series of <attribute>=<value> lines, and constitutes the body of a SIP message. The entities involved in the exchange of these messages are:

- SIP client: User Agent Client
- SIP server: User Agent Server
- Registrar Server (or Location Server)
- Proxy Server

The User Agent is the basic software component of a SIP stack. It is responsible for initiating and receiving messages, holding the data structures making up the client's state, as well as interfacing with the applications the stack supports.

The Registrar Server is similar to a lookup service; it associates each SIP address to one or more others. For instance, the SIP address, <sip:bob@pda.net>, is an alias for the real location, which may be <sip:bob@xyz.pda.net>. The association between these SIP URIs is held within the Registrar Server's database.

The Proxy Server acts in a way similar to an HTTP proxy; it forwards the requests it receives to the appropriate party, which it determines with the help of the Registrar Server. For example, when someone wants to call Bob, he will send a message to the Proxy Server at pda.net, requesting that <sip:bob@pda.net> gets called.

SDP is carried in MIME as a message body in SIP messages. A new MIME type called Device Message Protocol (DMP) has been defined [6] for this purpose. The DMP is an XML based format and used for conveying information pertaining to control, query and event subscription and notification functionality. DMP is intended to be carried as the body of the SIP. However, no assumptions are made on the encapsulating protocol, therefore, any protocol, which supports MIME types, such as HTTP, may also be valid for carrying DMP messages. When a message carries a DMP payload, the MIME type should be set to "application/dmp".

D. User Authentication

Authenticating SIP user is an important part of the system. the Notifier needs to verify the Subscriber subscribing to alert notifications. Also the Subscriber must authenticate the Notifier generating alerts messages.

SIP can use existing security mechanisms like HTTP Digest or transport layer security (TLS). Digest Authentication was originally built for HTTP authentication, and since SIP is quite similar to the HTTP protocol, it uses it as well. The most widely used algorithm for calculating digests and, therefore, providing challenges and responding to them, is the MD5 checksum [6], developed by R. Rivest and RSA Data Security, Inc. Digest authentication is built in such a way that it can verify that two parties know a shared secret, without actually communicating that secret either in plaintext or in an encrypted form on its own. It is based on a challenge-response paradigm: the server sends a challenge and expects a response that will only be valid if it uses the secret in its calculations.

When a SIP client sends a request to the Proxy or Registrar Server, the Server will check whether authentication is enabled for the particular user. Digest Authentication is not immune to attacks. In particular, a client can be a victim to a man-in-the-middle attack, whereby a fake server requests only basic authentication, or chooses a challenge that will easily lead to the password given the response sent from the client. On the other hand, replay attacks are not very likely, because of the timestamp which is included in the challenge [7].

HTTP Digest mechanism is used for authentication using a shared password, but it does not provide encryption of the messages. TLS is preferable for secure and encrypted SIP communication.

E. SUBSCRIBE-NOTIFY Mechanism

The SIP event notification [8] work defines two new methods, SUBSCRIBE and NOTIFY, that can be used to achieve asynchronous communications. When these two methods are used [8] with the MIME type payload, asynchronous event notification is established. Users subscribe to an event with the SUBSCRIBE method and receive notifications via NOTIFY. This event notification facility is used for events that occur during telephone calls for presence notification and also for generic SIP event notification systems. A user agent client sends a SUBSCRIBE request to the appropriate server. This request contains an "Event" header indicating the type of event the user is subscribing to. In the case where a user is interested in a number of events, it sends multiple SUBSCRIBE messages. The request's "Expires" header specifies the duration of the subscription. SUBSCRIBE messages can be refreshed whenever the subscription has expired. If a subscriber wants to unsubscribe, it can send a SUBSCRIBE message with an expiration time of zero.

SUBSCRIBE Mechanism involves,

- Naming and Routing
- Authentication of subscriber
- Acceptance/ rejection/redirection to subscription

NOTIFY Mechanism involves,

- Routing
- Correlation to subscription
- Authentication of its server
- Encryption

F. Security and Access Management

Security is a particularly important issue since the technologies described this project will be applied to the home

health care environments with personal and private information available online. At a minimum, message authentication and encryption are required to ensure that the SIP messaging system cannot be intercepted, modified, or copied. Supporting this type of functionality requires a fine degree of access control. There are also several kinds of attacks [8], which could take place in a SIP based event notification system. To prevent such attacks, implemented system requires proper user authentication mechanism. And at the same time information contained in the messages should be encrypted. SIP also provides a means of encrypting most portions of the message, including the payload, for end-do-end privacy.

Access Control

The ability to accept subscriptions should be under the direct control of the notifier's user, since many types of events may be considered sensitive for the purposes of privacy. Similarly, the notifier should have the ability to selectively reject subscriptions based on the subscriber identity, using standard SIP authentication mechanisms.

Notifier Privacy Mechanism

The mere act of returning a 200 or certain 4xx and 6xx responses to SUBSCRIBE requests may, under certain circumstances, create privacy concerns by revealing sensitive policy information. In these cases, the notifier should always return a 202 response. While the subsequent NOTIFY message may not convey true state, it must appear to contain a potentially correct piece of data from the point of view of the subscriber, indistinguishable from a valid response.

Denial-of-Service attacks

The current model (one SUBSCRIBE request triggers a SUBSCRIBE response and one or more NOTIFY requests) is a classic setup for an amplifier node to be used in a smurf attack. Also, the creation of state upon receipt of a SUBSCRIBE request can be used by attackers to consume resources on a victim's machine, rendering it unusable.

Replay Attacks

Replaying of either SUBSCRIBE or NOTIFY can have harmful effects. In the case of SUBSCRIBE messages, attackers may be able to install any arbitrary subscription which it witnessed being installed at some point in the past. Replaying of NOTIFY messages may be used to spoof old state information. The prohibition on sending NOTIFY messages to nodes which have not subscribed to an event also aids in mitigating the effects of such an attack.

Man-in-the middle attacks

Even with authentication, man-in-the-middle attacks using SUBSCRIBE may be used to install arbitrary subscriptions, hijack existing subscriptions, terminate outstanding subscriptions, or modify the resource to which a subscription is being made. To prevent such attacks, implementations should provide integrity protection across "Contact", "Route", "Expires", "Event", and "To" headers of SUBSCRIBE messages, at a minimum. Man-in-the-middle attacks may also attempt to use NOTIFY messages to spoof arbitrary state information and/or terminate outstanding subscriptions. To prevent such attacks, implementations should provide integrity protection across the "Call-ID", "CSeq", and "Subscription-State" headers and the bodies of NOTIFY messages.

Confidentiality

The state information contained in a NOTIFY message has the potential to contain sensitive information. It is also possible that the information contained in a SUBSCRIBE message contains information that users might not want to have revealed. Implementations may encrypt such information to ensure confidentiality. To allow the remote party to hide information it considers sensitive, all implementations should be able to handle encrypted SUBSCRIBE and NOTIFY messages.

VI. Future Work

Building the prototype of the proposed system and testing it in the real life environment should be the consecutive task, as the engineers mobility was the main issue of this project. The economical aspects of this designed system need to be investigated. It is also necessary to carry out the actual cost-benefit analysis before developing the system. SIP protocol is suitable for interacting with networked appliances across the Internet. Therefore study could be made to explore the secure remote control of networked BMD devices via the Internet. It could also be possible to establish a VOIP session between the patient and the hospital technician just after an alert notification message has reached to BMD technician. This will enable an interactive audio and video session, which will help the patient get an instant support from the technician.

VII. Conclusions

Due to the popularity of IP telephony and Internet communication increases in today's society, the necessity of providing a notification system on the Internet is becoming evident. SIP-based communication technology can open immense possibilities for the healthcare professionals. SIP based SUBSCRIBE-NOTIFY mechanism is relatively new technology, and still now few application systems have been developed and commercially available based on this mechanism. Therefore, it would be great to see a SIP based notification system developed and tested for the Telemed platform that will provide extra mobility to the hospital engineers at their work.

References

[1] Nabiev, Rustam, *Master Thesis: Telemedicine Services in Home Healthcare Sector*, IMIT, Royal Institute of Technology (KTH), MTA, Karolinska University Hospital (KUS), Stockholm, Sweden, December 2002.

[2] Jonsson Sven, Behovet av medicinteknisk support i framtidens hemsjukvård, Oral presentation at The Swedish Society of Medicine Annual General Meeting 2000. http://www.svls.se/sektioner/mtf/riksstamma-00.htm#Hemsjukvård (2004-05-14).

[3] Knarig Arabshian and Henning Schulzrinne, *"A SIP-based Medical Event Monitoring System"*, Department of Computer Science, Columbia University.

[4] Knarig Arabshian and Henning Schulzrinne, *"SIP-based Emergency Notification System"*, Department of Computer Science, Columbia University, October 2001.

[5] Handley, M., Schulzrinne, H., Schooler, E. and J. Rosenberg, "SIP: Session Initiation Protocol", IETF RFC 2543, March 1999.
[6] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", IETF RFC 2327, April 1998.
[7] R. Rivest, "The MD5 Message-Digest Algorithm", IETF RFC 1321, April 1992.
[8] RFC 3265 (rfc3265) - Session Initiation Protocol (SIP)-Specific Event Notification.