논문 2008-6-13

메디컬 그리드 장치를 위한 안전한 모바일 헬스케어 시스템에 관한 연구

A Study of The Secure Mobile Healthcare System for Medical Grid Devices

최규석*

Gyoo-Seok Choi

요 약 분산 컴퓨팅 환경에서 모바일 서로게이트 시스템은 보안상의 문제로 인하여 널리 사용되고 있지 못하고 있다. 현재 가장 널리 사용되고 있는 그리드 미들웨어인 글로버스에서도 모바일 단말기를 인증하는 방법이 제공되고 있지 않아 그리드의 강력한 컴퓨팅 능력을 모바일 클라이언트까지 확장하는 것을 어렵게 하는 중요한 요인이 되고 있다. 본 논문에서는 PDA와 같이 컴퓨팅 파워가 미약한 모바일 단말기기와 그리드 호스트 간의 인터페이스 역할을 하는 게이트웨이를 두고 모바일 클라이언트가 이동 중 그리드 서비스를 이용할 수 있도록 하는 안전한 모바일 그리드 서비스 프레임워크를 설계 구현하였다. 아울러, 이를 구현하여 ECG 신호처리를 위한 헬스케어 시스템에 적용하였다. 이 시스템은 이동 환경에서 환자의 생체 신호를 그리드 컴퓨팅으로 분석하여 원격에 있는 의료진이 진단할 수 있는 모바일 헬스케어에 활용가능하다.

Abstract The introduction of wireless information technology gives rise to new mobile services in all kinds of areas of out daily life. Mobile healthcare system is a production of composite ICT (Information and Communication Technology) which focused on signal sensing, processing, and communication in wireless environment. The mobile and wireless revolution promises not only expanded access to patient health information, but also improved patient care. In this paper, we describe a surrogate host based mobile healthcare information system which utilized Grid computing for real-time ECG signal processing. The surrogate host provides seamless interface between mobile device and Medical Grid portal. The security extension of GSI (Grid Security Infrastructure) allows mobile users to access Grid portal in a secure and convenient manner. The presented system architecture can be used as a secure enterprise mobile healthcare system for hospital physicians.

Key Words : Secure Mobile, Healthcare System, Grid portal, Distributed Computing

Ⅰ. Introduction

The introduction of wireless information technology gives rise to new mobile services in all kinds of areas of our daily life. Mobile healthcare system is a of composite ICT (Information and Communication Technology) which focused on signal sensing, processing, and communication in wireless environment.

The use of the PDA (Personal Digital Assistant) in a clinical setting has been gaining wide acceptance recently, with many reported advantages including a reduction in medical errors[1]. In order to build

*종신회원, 청운대학교 컴퓨터학과
(Dept. of Computer Science, Chungwoon University)
접수일자 2008.9.22, 수정완료 2008.12.4

distributed system that is highly adaptive to change, a distributed object middle-ware that allows objects to inter-operate across networks regardless of the language is required.

The tow most dominating distributed object technologies or middle-ware CORBA (Common Object Request Broker Architecture) of OMG (Object Management Group) and DCOM (Distributed Component Object Model) by Microsoft, respectively.

However, they are not prepared to offer proper support for addressing the dynamic aspects of mobile systems.

Modern distributed applications need a middle-ware that is capable of adapting to environment changes and that supports the required level of quality of service. Java RMI overcomes the problem by allowing a client to obtain the stub from the server at runtime.

Jini is new network 'ping and play' technology based on Java, which allows software and hardware or software component to join a network of Jini technology-enabled services, it must satisfy several critical requirements: it must be able to participate in the Jini discovery and join protocols, and it must be able to download and execute classes written in the Java programming language. In addition, it may need the ability to export classes written in Java programming language so that they are available for downloading to remote entity.

For many hardware or software components, these requirements are not difficult to meet[2]. Jini Surrogate is designed to address this problem by defining a means by which these components, with the aid of a third party, can participate in a jini network while maintaining the plug-and-work model of Jini network technology.

In the paper, we have designed a surrogate host based mobile healthcare information system which utilized Grid computing for real-time patient's ECG signal processing. In order to provide secure communication between mobile devices and Grid portal, we have extended the GSI [3][4] functionality since PDA dose not have enough computing power and storage space to download and install distribution package of associated CA (Certificate Authority).

The rest of this paper is organized as follows. The background and related work is summarized in Section2. Section 3 describes implementation of the proposed surrogate host based mobile healthcare system. Conclusions are presented in Section 4.

II. Related work

2.1 Surrogate Host System

The Jini surrogate architecture provides both the necessary facilities to implement communication gateways for interconnections, as well as a place where processing power can be apportioned to a surrogate that acts on behalf of an attached device. Using the surrogate architecture, devices that not directly connected to a Jini network, or are otherwise unable to have direct access to the Jini technology infrastructure, can supply surrogate that can access the Jini network and have access to the Jini technology infrastructure.

These surrogate represent, and act on the behalf of the device that is not Jini technology-enabled[2]. A surrogate host is an environment specially designed for the hosting of surrogates. Surrogates can be loaded into a surrogate host and executed. The key surrogate modules include discovery, retrieval and loading of surrogate, execution, and live-ness monitoring. In order to realize the surrogate architecture, there must exist a host-capable machine connected to the device interconnect and the Jini network. Furthermore, the host-capable machine must be able to execute code written in Java on behalf of the device and supply the resources that such code may need.

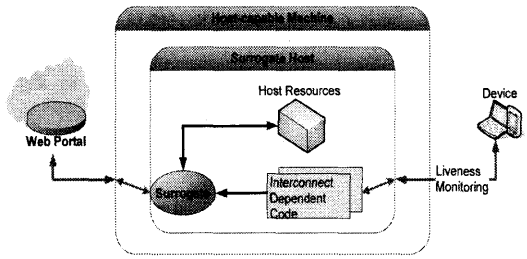

Fig. 1. Architecture of Surrogate System

The surrogate host resides in a host-capable machine and can be seen as a Jini gateway. Morever, there is an interconnect adapter monitoring the device interconnect. The brief surrogate architecture is shown in figure 1.

2.2 Security of Mobile Grid

Recently, there is a growing rank of mobile users equipped with mobile phones and PDAs which have limited computing power as well as frequent disconnected state. When such a user needs to perform some computation intensive task, the user should connect to an application server as a client and remain connected until the results are obtained. In order to provide mobile Grid computing to mobile devices, various mechanism are proposed in the literature[5-7].

Most of them use the mobile agent technologies to provide a powerful computing platform to mobile client applications that can migrate from the client machine to the networked host system. The mobile agent can carry out the computation while the client system remains disconnected.

The client can retrieve the results at a later convenient time or can be notified by the agent through paging if timing is crucial. However, mobile agent approach would cause some security and trust problem because the hosts are no longer belong to only one user or organization in grid environment. To address those security issues brought from multiple organizations, GSI has established a framework by which general authentication and authorization can be carried on[7].

GSI enables a job to access local and remote resources securely. The surrogate host system proposed in this paper can be viewed upon as a midway approach between the traditional client server architecture and the full-fledged mobile agent based architecture, and combines the advantages of both in a useful manner. It just extends the GSI-based security mechanism to wireless domain, which serves to extend the computing power of the end user devices allowing the flexibility of disconnected operation.

At the same time it largely eliminates the complex security concerns of the mobile agent approach by sticking effectively to the safer client-server model of computation.

2.3 MyProxy

MyProxy is open source software for managing X.509 Public key Infrastructure (PKI) security credentials which include both certificates and private keys. MyProxy combines an online credential repository with an online certificate athority to allow users to securely obtain credentials when and where needed.

Users run MyProxy log-on to authenticate and obtain credentials, including trusted CA certificates and Certificate Revocation Lists (CRLs). The motivation for MyProxy is its usability on Grid portals. Grid portal is a suitable framework to integrate Grid resources and help users communicate easily with the Grid infrastructure via web browers.

Grid portal requirements are:

- Users must be able to use any standard web browsers to access Grid portals
- Users must be able to use a web browser from any location
- Users must be able to do anytihng through the Grid portal their credentials would normally entitle them to.

However, the current off-the -shelf web browsers do not support delegation of credential. This prevents

the portal from being able to act as the user without being given a permanent copy of the user's credentials. Credentials are not securely available everywhere, normally stored on disk at the user's home site. Portal needs to use the same credential user would normally use.

The portal could have an alternate set of credentials for the user, but this gets into scalability problems as the number of identities for the user grows. Thus, MyProxy system is designed to allow users to access their credentials from anywhere on the Grid and users to delegate credentials to resources to which they normally would not be able to. Credentials should only exist on the portal when they are actually needed. For scalability multiple portals should be able to use a singe MyProxy system. A portal should be able to use multiple MyProxy systems and user should retain as much control of their credentials as possible.

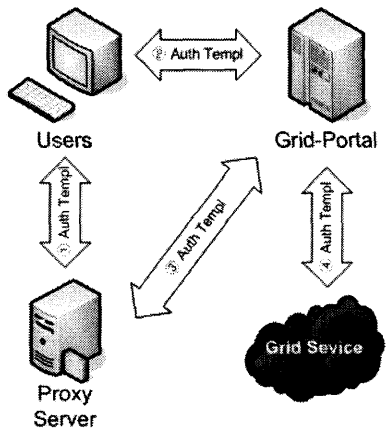

Fig. 2. User connecting to portal and portal interaction with MyProxy server

MyProxy system consists of a MyProxy server and a set of client programs. The server stores and protects credentials and client programs run by the user and the portal interact with the server to store and retrieve credentials. To user MyProxy system with a portal, a user delegate a proxy credential to the MyProxy server as shown in figure 2.

Ⅲ. Implementation

3.1 System Architecture

The proposed surrogate host based mobile healthcare system consists of four types of hosts: mobile device (PDA), surrogate host, Grid portal, and MyProxy server as shown in figure 3.

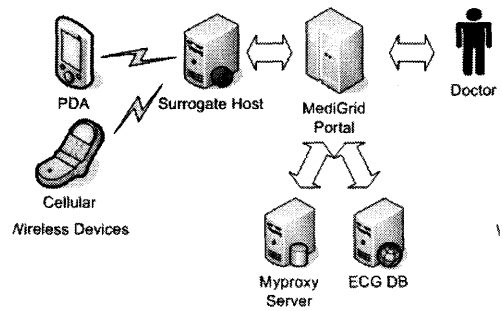

Fig. 3. Architecture of Mobile Healthcare System

Surrogate host is located between wireless network and Grid portal. It provides two different services to mobile devices: relay and access control. First it accept PDA client's service request and verifies the mobile user, and relays the request to the Grid portal. Second, it performs access control to verify mobile user to access associated Grid portal.

MyProxy server allows users to access their credentials from anywhere on the Grid and users to delegate credentials to resources to which they normally would not be able to. Credentials should only exist on the portal when they are actually needed. MyProxy system consists of a MyProxy server and a set of client programs.

The server stores and protects credentials and client programs are executed by the user and the portal interacts with the server to store and retrieve credentials. To use MyProxy system with a portal, a user delegates a proxy credential to the MyProxy server. Then, at different location and different time, the user connects to the Grid portal using a web browser and authentication information such as user id and pass phrase.

The portal would connect to the MyProxy server, and presents the authentication information provided by the user, and requests a proxy credential for the user. The proxy server verifies received information, and provides a proxy credential back to the portal. The portal can now use the credential to access the Grid on the user's behalf using standard Grid applications and tools. Server scenario of the surrogate host system can be summarized as follows. A mobile user executes a healthcare client in his PDA using his registered id and pass phrase, and sends connect request to surrogate host.

Then surrogate host verifies the user's authentication information utilizing re-registered database information. Surrogate host relays the connect request to Grid portal.

If connection is successful, *myproxy-init* activation is displayed on PDA. Once the user activates *myproxy-init*, this request is relayed to MyProxy server via Grid portal. The proxy server verifies received information, and provides a proxy credential back to the PDA via Grid portal. Finally, the mobile user can access Grid healthcare services using the proxy credential. Now the mobile healthcare user is ready to send his ECG signal to Grid portal for analysis.

ECG data sensing is not considered in this paper, but we assume that ECG signals are stored in user's PDA. As real sample ECG signals, we use MIT-BIH Arrhythmia Database[8-11] in Physiobank. The MIT-BIH Arrhythmia Database contains 48 half-hour excepts of two-channel ambulatory ECG recordings.

If PDA user sends ECG signal to Grid portal via surrogate host, the signal is analyzed using signal processing algorithms. For real-time signal processing GT (Globus Toolkit) 4 based Grid computing has been adopted.

Once the ECG signal is analyzed, various parameters such as RR interval and ST segment are obtained to estimate possible heart symptoms such as arrhythmia. These parameters and ECG waves are transmitted to physician in order to diagnose patient's heart for possible heart problems. After examining patient's ECG associated data, the physician would notify what has happened with the patient's heart for proper care via Medical Grid portal.

3.2 Mobile Device Monitoring

Once a surrogate is loaded and activated, the surrogate host monitors the mobile device for live-ness. Live-ness means that a usable communication path exists between the surrogate and the device that ti represents, and that both entities are active. If the device is no longer reachable for any reason (e.g. due to a network failure), then the surrogate is deactivated by the surrogate host to release any resources being used. The surrogate has to de-register with the Jini lookup service to let the service users being notified about the disconnected service.

The device service determines that the device is no longer connected the surrogate host, so it can try to re-establish the interconnection when possible.

Live-ness monitoring of surrogate is implemented to monitor and maintain the status information of mobile devices. When the PDA connects to the surrogate host for the first time, it sends periodically static information associated with CPU, memory, storage, device type, and operating system. It also periodically reports non-static information such as live-ness, id, ip address, port number, and current status to the surrogate host. Figure 4 shows the log-based PDA monitoring procedure.

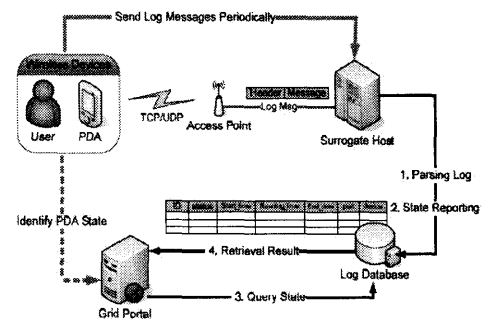

Fig. 4. Log-based PDA Monitoring

3.3 Analysis of ECG Signals

Patient's ECG signal is transmitted to Grid portal via surrogate host processed in real-time to extract ECG features such as R-R interval, QRS duration, and ST segment based on Grid computing. The extracted ECG parameters along with ECG waves in time domain can be transmitted to physician's terminal or the doctor can access the Grid portal to examine the ECG data and produce medical opinion for the patient.

Figure 5 shows three-channel ECG signals and extracted features implemented by the Java applet (JDK ver. 5.0).

The extracted features are classified into four different categories: segment, duration, interval, and amplitude. If the average value of resulting features ranges within the pre-defined values, the patient is assumed to be normal for the specific measurement.

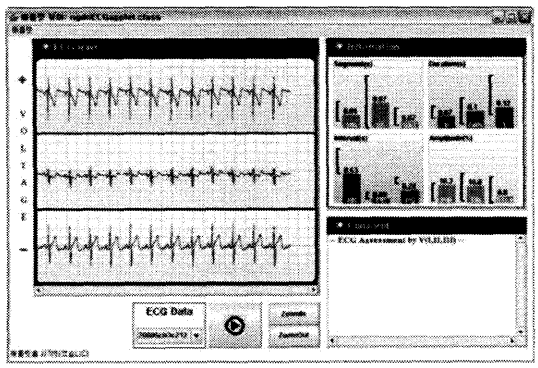

Fig. 5. ECG Signal & Extracted Features

These ECG related features would be considerably helpful for the doctor to diagnose patients. After examining patient's heart data, doctor adds his medical opinion in comments box which located at right bottom corner of figure 5.

Once doctor's medical opinion is stored in the portal, the portal can transmit the medical information to patient's PDA or request the patient to access the portal to retrieve the doctor's opinion for appropriate reaction.

Ⅳ. Conclusions

We have presented a mobile healthcare system prototype based on surrogate host system. the surrogate host provides seamless interface between mobile device and Grid portal. For security the proxy based GSI is extended to provide authentication of wireless devices.

In addition, the surrogate host relays PDA's request to the portal, manages user session, and Provides log-based PDA monitoring. The experimental results showed that the developed system could be utilized to provide patients with real-time heart disease diagnosis based on Grid computing in a secure and convenient manner.

This investigation proved that Grid-based healthcare services could be extended from desktop environment to the mobile domain.

References

[1] C. Pavlovski, H. S. Kim and D. Wood, "Ubiquitous Mobility in Clinical Healthcare", In Proc. of the IDEAS Workshop on Medical Information System: Digital Hospital, 2004.

[2] Surrogate System, http://surrogate.jini.org

[3] http://www-unix.globus.org/toolkit/docs /3.2/security.html.

[4] D. Kouril and J. Basney, "A Credential Renewal Service for Long-Running Jobs", In Proc. of the 6th IEEE/ACM International Workshop on Grid Computing, 2005.

[5] Amitabha Das, "A Scalable and Secure mobile Agent Based Surrogate Host System", In Proc. of IEEE Region 10 International Conference on Electrical and Electronic Technology, TENCON, 2001.

[6] H. K. Neo, Q. P. Lin and K. M. Liew, "A Grid Based Mobile Agent Collaborative Virtual Environment", In Proc of International

Conference on Cyber Worlds, 2005.

[7] T. Ma and S. Li, "An Instance-Oriented Security Mechanism in Grid based Mobile Agent System", In Proc. of IEEE International Conference on Cluster Computing, 2003.

[8] http://www.physionet.org/physiobank /database/mitdb/.

[9] Huang H. K, Brent J, Liu, Zheng Zhou, Jorge Document, "A Data Grid Model for Combining Teleradiology and PACS Operations", In Med ImageTech, 2006.

[10] Foster, I., C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International Journal of Supercomputer Applications, 2001.

[11] Novotny, J., and V. Welch., "An Online Credential Repository for the Grid: MyProxy", In High Performance Distributed Computing, 2001.

저자 소개

최 규 석(종신회원)

- 1982년 연세대학교(전기전자) 공학사
- 1987년 연세대학교(전기전자) 공학석사
- 1997년 연세대학교(전기전자) 공학박사
- 1987년 1월~1997년 1월 (주)데이콤 정보통신연구소 연구원 및 (주)SK텔레콤 중앙연구원 책임연구원 근무, 1997년 ~현재 청운대학교 컴퓨터학과 교수

<주관심분야 : 인공지능, 데이터통신 및 이동통신, 인공생명, ITS, Mobile Computing 등>