A Study of a Secure Mobile Agent Services Based on Grid Proxy Gateway

Se-Yul Lee, Gyoo-Seok Choi, Chang-Su Kim and Hoe-Kyung Jung, *Member, KIMICS*

Abstract— In distributed computing paradigm, mobile surrogate systems migrates from on host in a network to another. However, Mobile surrogate system have not gained wide acceptance because of security concerns that have not been suitably addressed yet. In this paper, we propose a security framework based on Grid Proxy Gateway for mobile Grid service. The current Grid Security Infrastructure is extended to mobile computing environments. The surrogate host system designed for mobile Personal Digital Assistant (PDA) users can access the certified host and get his proxy credential to launch remote job submission securely.

Index Terms— Distributed Computing, Grid Security, Mobile Agent, Proxy Grid Gateway.

I. INTRODUCTION

Grid computing was originally conceived by research scientists as a way of combining computers across a network to form a distributed super-computer to tackle complex computations. Large-scale Grids are widely used in scientific and academic computing. Grid portals are a common approach to providing user interfaces to grid applications. By combining a web server and Grid-enabled software, a Grid portal allows the use of standard web browser as a single graphical client for Grid applications.

Most Grid portals require that the user delegate to the server the right for that server to act on the user's behalf in order to initiate and monitor operations for that user on Grid resource [1]. Grid Security Infrastructure [2], that is a set of libraries and protocols that allows users to access Grid resources securely, has been used to protect such Grid resources. In order to provide web-security with delegation capability, and online credential repository, called MyProxy, was developed by [3].

MyProxy enables grid portals to use Grid Security Infrastructure-protected resources in a secure, scalable manner. MyProxy combines an online credential repository with an online certificate authority to allow users to securely obtain credentials when a where needed.

Manuscript received April 12, 2008; revised August 8, 2008. Se-Yul Lee is with the Department of Computer Science, Chungwoon University, Chungnam, 350-701, Korea (Tel: +82-41-630-3225, Fax: +82-41-634-8700, Email: pirate@chungwoon.ac.kr)

Grid computing technology is being extended to mobile environments, in which enables any device to access or provide the required computing power, information or other services from or to the Grid.

In this paper, we have extended the Grid Security Infrastructure functionality for secure authentication and communication to mobile Grid device such as PDA since PDA dose not have enough computing power and storage space to download and install distribution package of associated Certificate Authority (CA) [4]. This security extension allows mobile users to access Grid computing environments in a secure and convenient manner. In order to provide seamless interface between mobile device and certified Grid host, a surrogate host system, called Grid Proxy Gateway, is designed.

The rest of this paper is organized as follows. The background and related work is summarized in Section 2. Section 3 describes the proposed surrogate host architecture and implementation. Conclusions are presented in Section 4.

II. BACKGROUND AND RELATED WORK

A. Grid Security Infrastructure

Grid Security Infrastructure is the Globus Toolkit 4 (GT4) component that addresses all these requirements and allows for privacy, integrity, and replay protection for Grid communication to eliminate sniffing and man-in-the-middle attacks, as well as single sing-on (SSO) and delegation abilities for Grid users. It also includes facilities for verifying the identity of a Grid entity authentication and authorization. Grid Security Infrastructure implements standards from various standards bodies and specifications from the web server community to provide the fundamental security needs. GT4 security is composed of both web services based and non web services based elements that together realize Grid security.

Grid Security Infrastructure has been traditionally based upon public key encryption for all its functionalities. It uses X.509 end-entity certificates for establishing identities of persistent entities, such as users and resources. It also introduces the notion of X.509 proxy certificates, which support delegation and the establishment of identities for temporary and often short lived entities. Grid Security Infrastructure treats both of the certificate types equivalently. Grid Security Infrastructure makes use of Secure Sockets Layer (SSL) to achieve secure communication between Grid entities.

SSO is important feature for Grid applications which

enables easy coordination of multiple resources. SSO is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems. To support SSO Grid Security Infrastructure adds the following functionality to SSL: Proxy credentials and credential delegation.

Proxy credentials are short lived credentials created by user, which is a short term binding of user's identity to alternate private key. The credentials are stored unencrypted for easy repeated access, and has a short life time in case of theft. This feature of credentials enables user to authenticate once then perform multiple actions without re-authenticating.

On the other hand, Grid Security Infrastructure enables user to create and delegate proxy credentials to processes running on remote resources, which allows remote processes and resources to act on user's behalf. Delegation is important for complex applications that need to use Grid resources, e.g. jobs that need to access data storage.

B. Host-capable Machine

The 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 attacked device. Using the surrogate architecture, devices that are not directly connected to a network, or are otherwise unable to have direct access to the technology infrastructure, can supply surrogates that can access the network and have access to the technology infrastructure. These surrogates represent, and act on the behalf of the device that is not technology-enabled [5]. A surrogate host is an environment specially designed for the hosting of surrogates. Surrogates can be loaded into a surrogate host and executed.

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

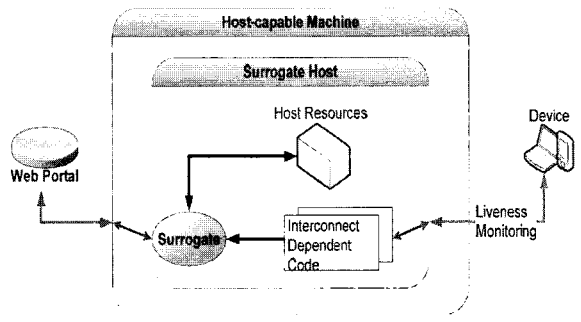


Fig. 1 Host-capable Machine Architecture

C. 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 authority 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 browsers.

Grid portal requirements are:

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

However, the current off-the-shelf web browsers do not support delegation of credentials. 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 single MyProxy system. A portal should be able to use multiple MyProxy systems and user should retain as much control of their credentials as possible.

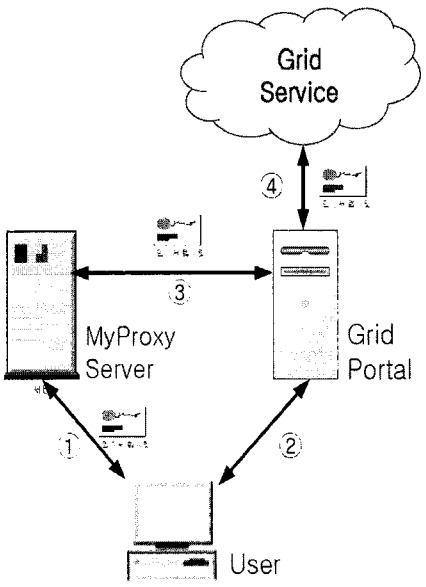


Fig. 2 User connecting to portal and portal interaction with MyProxy server

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 Fig. 2. 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.

D. 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 the surrogate host systems are proposed in the literature [6-10]. 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 on user or organization in Grid environment. To address those security issues brought from multiple organizations, Grid Security Infrastructure has established a framework by which general authentication and authorization can be carried on [7, 11, 12]. Grid Security Infrastructure 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 Grid Security Infrastructure based security mechanisms 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.

III. SURROGATE HOST SYSTEM

A. System Architecture

The proposed surrogate host system for mobile Grid service consists of four types of host: mobile device (PDA), Grid Proxy Gateway (GPG), Grid Host (GH), and MyProxy server as shown in Fig. 3, 4. GPG is located between wireless network and wired Grid network. 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 GHs, vice versa. Second, it performs access control to verify mobile user to access associated GHs.

Initially the Grid host has a host certificate and the user also maintains user certificate issued by the CA server, respectively, based on PKI. Service scenario of the surrogate host system can be summarized as follows.

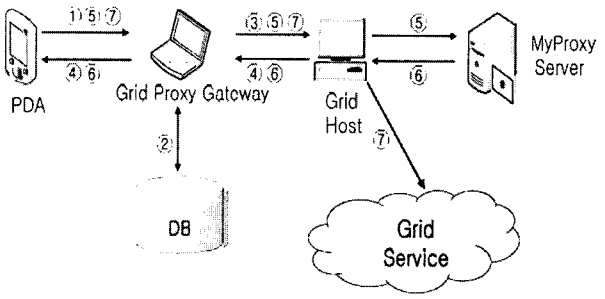


Fig. 3 Surrogate Host System for Mobile Grid

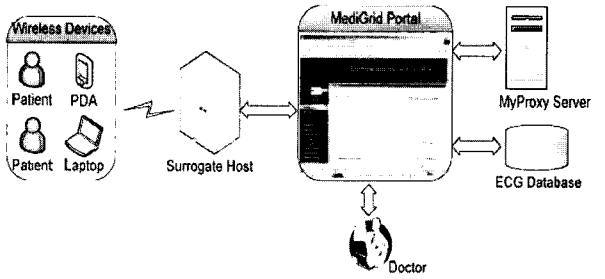


Fig. 4 Mobile healthcare System

A mobile user executes GPG client in PDA using his registered ID and pass phrase, and sends connect request to GPG (①). GPG verifies the user's authentication information utilizing pre-registered DB (②). GPG relays the connect request to user's own Grid host (③). If connection is successful, myproxy-init activation button is displayed on PDA (④). Once the user activates myproxy-init, this request is relayed to GH via GPG, and GPG sends myproxy-init command to MyProxy server (⑤). The proxy server verifies received information, and provides a proxy credential back to the GH. Receiving proxy credential from MyProxy server, GH sends verification message to GPG, and GPG relays this message to PDA (⑥). Finally the mobile user can access Grid services using proxy credential stored in GH (⑦). For example, 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 pre-registered DB 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, we Use MIT-BIH Arrhythmia Database in Physiobank [13]. The MIT-BIH Arrhythmia Database contains 48 half-hour excerpts 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 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 Medi-Grid portal.

B. Implementation

For mobile Grid services we have extended the GT 4 based wired Grid infrastructure. The two newly added hosts are a secure surrogate host, named GPG, and mobile device, PDA. A prototype of GPG server was built on Windows XP based host using Java 2 Platform Standard Edition (J2SE), while GPG client was developed on HP iPAQ rx3700 PDA running IBM J9 VM for palm devices. The detailed software components and interactions for authentication among PDA, GPG, and Grid host are described in Fig. 5.

The developed surrogate host system was tested in Grid test-bed as shown in Fig. 3, 4. Fig. 6 shows log in window when mobile user executes GPG client from HP PDA, while Fig. 7 shows proxy verification message which is relayed from Grid host via GPG. This new proxy credential can be verified by comparing its proxy creation time with Grid host's proxy creation time.

The test results of this surrogate host system have proved that a lightweight standard based PDA client can be developed to access Grid resources securely. By combining the HP PDA with an IEEE 802.11b wireless network card the J2ME compliant GPG client developed in the work can access a Grid using standard application environment and network protocols.

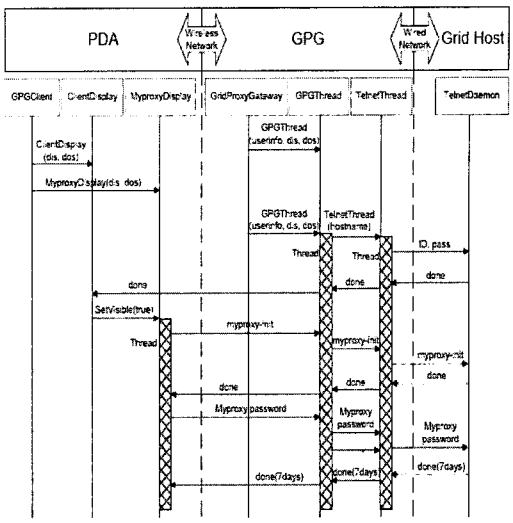


Fig. 5 Interactions among PDA, GPG, and Grid host

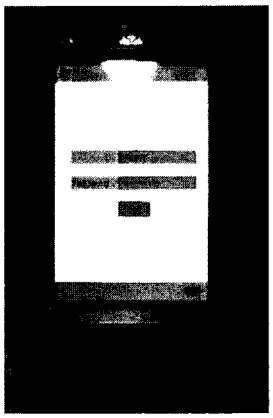


Fig. 6 Log in window

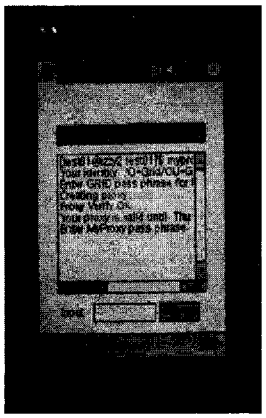


Fig. 7 Authentication window

IV. CONCLUSIONS

In this paper, we proposed a secure surrogate host system which enables a mobile user to access Grid host from PDA which does not have enough computing power and storage space to run distribution package of associated CA.

We have designed and implemented a surrogate host, named GPG, in order to provide proxy based authentication between PDA and Grid host. The experimental results on the test-bed showed that the developed GPG verifies mobile user and provides proxy credential verification message to mobile user in a convenient and secure manner. This investigation proved powerful Grid services, called Grid based healthcare services could be extended from desktop environment to the mobile domain.

REFERENCES

[1] Jason Novotny and Steven Tuecke, "An Online Credential Repository for the Grid: MyProxy," In Proc. Of 10th IEEE International Symposium on High Performance Distributed Computing, pp. 104-111, Aug. 2001.

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

[3] GT 4.0: Credential Management: MyProxy, http://www.globus.org/toolkit/docs/4.0/security/myproxy/

[4] GT 4.0: Credential Management: SimpleCA, http://www.globus.org/toolkit/docs/4.0/security/simpleca/

[5] Surrogate Host, http://surrogate.jini.org/

[6] Amitabha Das, "A Scalable and Secure Mobile Agent Based Surrogate Host System," In Proc. Of 10th International Conference on Electrical and Electronic Technology, pp. 776-782, Aug. 2001.

[7] H. K. Neo, Q. P. Lin and K. M. Liew, "A Grid Based Mobile Agent Collaborative Virtual Environment," In Proc. Of International Conference on Cyberworlds, pp. 335-339, Nov. 2005.

[8] 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, pp. 492-495, 2003.

[9] K. Ohta et al, "Design and Implementation of Mobile Grid Middleware for Handsets," In Proc. Of 11th International Conference on Parallel and Distributed Systems, pp. 679-683, July. 2005.

[10] H. S. Cho, B. H. Lee, M. K. Kim, S. Y. Lee, and C. H. Youn, "A Secure Mobile Healthcare System Based on Surrogate Host," In Proc. Of 6th IEEE International Conference on Computer and Information Technology, pp. 101-106, Sept. 2006.

[11] John Brooke and Michael Parkin, "A PDA client for Computational Grid," In Proc. Of 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, pp. 325-330, June. 2005.

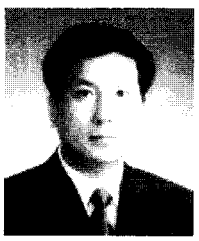
[12] Dario Bruneo, Marco Scarpa, Angelo Zaia, and Antonio Puliafito, "Communication Paradigms for Mobile Grid User," In Proc. Of 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 669-676, May. 2003.

[13] Physionet Physiobank Database MIT-BIH, http://physionet.org/physiobank/database/mitdb/

Se-Yul Lee
received the M. S. Degree in Department of Information and Communications Engineering and Ph. D. degree in Department of Computer Engineering form Daejeon University, in 1999 and 2003, respectively. He was a researcher at Insopack Ltd and ETRI from 2000 to 2003. Since 2004 he has been a Full-time Lecturer in Department of Computer Science at Chungwoon University. His current research interests include Network Security, Intrusion Detection and Prevention, Grid middleware, and Fuzzy Neural Networks.

Gyoo-Seok Choi
received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Yonsei University, Seoul Korea, in 1982, 1987, and 1997, respectively. He worked at the laboratory of DACOM Company as a researcher from 1987 to 1990. He also worked at the laboratory of SK Telecom Company as a senior researcher from 1991 to 1996. He is currently Associate Professor in the Department of Computer Science. His current research interests include Artificial Intelligence, Telematics, Mobile Computing, etc.

Chang-Su Kim
received the B.S., M. S. and Ph.D. degrees in computer engineering from PaiChai University, in 1996, 1998 and 2002, respectively. From 2001 to 2004, he was a lecturer of Paichai University, IT Education Center. Since 2005, he has worked as a Full-time lecture in Department of Internet at Chungwoon University. His current research interests include Document Information Processing, web service, Mobile Internet Service.



Hoe-Kyung Jung
received the B.S., M. S. and Ph.D. degrees in computer engineering from Kwangwoon University, in 1985, 1987 and 1993, respectively. Since 1994, he has worked as a professor in Department of Computer Engineering at PaiChai University. His current research interests include XML, semantic web, MPEG-21, Mobile RFID.