J Med Syst (2013) 37:9947
DOI 10.1007/s10916-013-9947-2

ORIGINAL PAPER

Secure Mobile Agent for Telemedicine Based on P2P Networks

Wen-Shin Hsu · Jiann-I Pan

Received: 12 February 2013 / Accepted: 7 April 2013 / Published online: 19 April 2013

Abstract Exploring intelligent mobile agent (MA) technology for assisting medical services or transmitting personal patient-health information in telemedicine applications has been widely investigated. Conversely, peer-to-peer (P2P) networking has become one of the most popular applications used in the Internet because of its benefits for easy-to-manage resources and because it balances workloads. Therefore, constructing an agent-based telemedicine platform based on P2P networking architecture is necessary. The main purpose of this paper is to construct a safe agent-based telemedicine that based on P2P networking architecture. Two themes are addressed in this paper: (a) the P2P network architecture for an agent-based telemedicine service, and (b) the security mechanisms for the proposed telemedicine networking architecture. When an MA contains patient information and migrates from one host to another through the Internet, it can be attacked by other software agents or agent platforms that can illegally access patient information. The proposed P2P network architecture is based on the JXTA protocol and provides two types of telemedicine service models: the predictable service model and unpredictable service model. This architecture employs a two-layer safety mechanism for MAs (i.e., time-limited black boxes and RSA undetachable signature technologies), to provide a secure solution for agent-based telemedicine services.

Keywords Telemedicine · Mobile agent · Time-limited black boxes · RSA-undetachable signatures

W.-S. Hsu
Institute of Medical Science, Tzu Chi University,
Hualien, Taiwan, Republic of China
e-mail: 95351114@stmail.tcu.edu.tw

J.-I. Pan (✉)
Department of Medical Informatics, Tzu Chi University,
Hualien, Taiwan, Republic of China
e-mail: jipan@mail.tcu.edu.tw

Introduction

Because of the advancement of medical and computer network technology, telemedicine is growing quickly and steadily. Telemedicine refers to the use of electronic information and communication technologies that provide and support health care when distance separates the users [1]. Telemedicine has the potential to enhance the accessibility and quality of health care delivery and lower costs [2]. Telemedicine refers to the delivery of health care using computers and telecommunication technology for diagnosis and treatment. Whenever appropriate, diagnosis and treatment during the course of patient interactions can be achieved remotely. The telemedicine contains a variety of application types, including tele-consultation, tele-education, tele-monitoring, and tele-surgery. They have one common characteristic, i.e., the link with the communication between the service provider and the service requester is the peer-to-peer relationship [3, 4].

As advocated by numerous researchers, mobile agents (MAs) are widely recognized as facilitating medical and telemedicine applications [5–8]. MA has the properties of autonomous, reactive, and/or proactive natures; their ability to apply negotiation strategies when a decision is required; their collective communicative skills; and the learning mechanisms that can be embedded in them. An MA is efficient in diverse computer network applications because of its autonomy and capacity for adaptation. MAs operate in computer networks and are capable of moving from server to server as required to fulfill their goals [6]. These properties can facilitate the telemedicine implementation and deployment in an efficiency way.

On the other hand, MAs are suitable for designing peer-to-peer (P2P) systems because an MA can travel across the nodes of a P2P network to discover peers and their resources [9, 10]. When programmed to perform a task, MAs can execute it autonomously on remote sites without intervention

from their own originating site. In addition, MAs can obtain patient information, such as patient IDs, names, addresses, telephone numbers, and conditions, through P2P networks.

However, MAs are increasing the patient security risk in P2P-based telemedicine, due to the attacks from Internet or malicious agents [9, 11, 12]. Therefore, patient privacy, security, availability, reliability, and time limitation issues must be considered in the security architecture of agent-based telemedicine. For this paper, we proposed four security requirements for telemedicine based on P2P networks [5, 13–16]:

1. Confidentiality: Patient privacy
2. Integrity: Patient data security
3. Reliability: Real-time
4. Non-repudiation: Medical information and service non-repudiation.

In this paper, we propose a hybrid approach for integrating an undetachable signatures approach, time-limited black boxes [9], and timestamp mechanisms. The hybrid security approach is exemplified by an MA-based emergency service application. The remainder of this paper is organized as follows. The following section presents related works on this subject. In Section Telemedicine service on P2P network, two types of telemedicine service models are considered. Section Secure Mobile Agent for Telemedicine based on P2P Networks shows the security model design developed on a P2P network. Finally, concluding remarks are offered in Section Conclusion.

Related works

This section provides a brief explanation of both MA and P2P technologies.

Mobile agents

MA technology has existed for several years, and is an effective means of dynamic distributed computing [6]. An MA is a mobile code: Namely, a code that can be transferred over the network and executed on another computer is combined with the properties of an MA. Thus, an MA can communicate with other agents and can take active or reactive measures regarding outside events. An MA is a mobile code that acts autonomously on behalf of a user for the continuous collecting, filtering, and processing of information. MAs must be prepared to function on various hosts in which, according to specific environmental conditions, they adopt differing behaviors.

Software agent-based healthcare systems have been developed in many telemedicine service areas. For examples, Koutkias [8] proposed an intelligent agent-based home care system for chronic diseases patients. Huge data related to the care of patient can be analyzed and delivered to physician who located in hospital by multiple agent cooperation. Mea [17] use of multiple software agents to establish a long-distance medical education system, named TOMAS (Telemedicine-Oriented Medical Assistant). Software agents can establish connection with hospitals to access the relevant medical information, or link to Medline digital online library for querying needed medical knowledge.

P2P networks

The JXTA project is an effort by Sun Microsystems to standardize P2P development. It is an open-source development effort that uses XML to encode and expose the availability of resources on the P2P networks that use this framework [18]. Using the JXTA shell and components, developers can create a number of emerging standard P2P services, including instant messaging, collaboration, and content management. JXTA peers create a virtual network where any peer can interact with other peers and resources directly, despite certain peers and resources existing behind firewalls or using different network transports [13].

P2P networks are popular subjects of research because they offer an easy strategy for managing distributed resources, such as storage space or processing power [5, 19, 20]. For instance, users must install one client for file sharing, an additional client for distributed computing, another for instant messaging, et cetera. For example, users cannot share files between SKYPE and MSN messaging services.

With the increasing demand for web-based services, the traditional client–server paradigm is being replaced by the P2P paradigm in which clients interact with each other for real-time collaboration and information sharing in a large-scale environment [21].

The JXTA community is considering a security model that relies on existing trusted technologies that do not compromise the strong security that users and enterprises expect from traditional computing approaches. This type of approach is practical because of three recent choices by the Project JXTA team [22–24]:

- Adoption of a transport layer security, which is an emerging industry protocol for the secure transport of information.
- Exploitation of the JXTA protocol end-to-end transport independence.
- Use of X509 Version 3 digital certificates in a manner that neither mandates nor excludes centralized certificate authorities.

Telemedicine service on P2P network

Each peer plays the role of both "server" and "client;" easing the implementation of MA services is critical. We demonstrate that by using JXTA API every peer can easily initialize, execute, and terminate agents. The proposed P2P network architecture that is based on the JXTA protocol uses two telemedicine service model types: the predictable service model and the unpredictable service model.

Predictable service model

The first model is predictable and includes tele-surgery, tele-education, and tele-consultation being performed online by two hospitals for the purpose of clinical teaching. In these processes, a member in the peer group can provide services, and the required services for all peers are defined in advance. When Hospital B performs a tele-surgery, it renews the announcement immediately, alerting all members in the peer group to the message. If Hospital A desires to participate, then Hospitals A and B can perform the tele-surgery by instantly delivering images and data. Figure 1 shows the predictable model.

When Hospital B desires to perform a catheterization, the surgical operation time is published in an advertisement for participating doctors and nurses, enabling the peers in this peer group to receive the message. When Hospital A desires to participate, it must send a message to Hospital B by posting a message regarding participation on the tele-surgery module. Hospital B then sends all of the tele-surgery data, including patient information, images, and other related data to Hospital A. In addition, all data must use the time-limited black boxes and RSA undetachable-signatures method for protection.

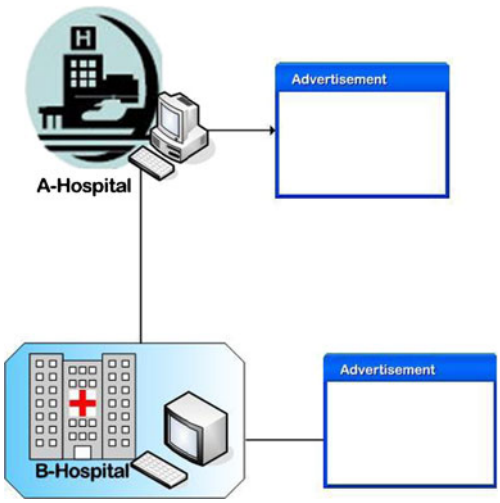

Fig. 1 An example of predictable model

Peer advertisements include peer-IDs, group-IDs, names, dates, times, and interventional surgeries [16] (see the Fig. 2).

- Peer-ID: This ID identifies a class of modules.
- Group-ID:
- Name: the hospital's name.
- Date: the surgery date.
- Time: Time of surgery.
- Interventional surgery: A type of the surgery.

Unpredictable service model

The second model is unpredictable and includes the following: public hygiene education; emergency-room resources; all peers must announce what services they can provide, and registered in the service management center of local area (e.g., the Emergency Service Center in Fig. 3). This paper used an urgent medical treatment service for emergency room resource application as the example of the unpredictable service model. Figure 3 shows a telemedicine system based on a P2P network.

First, each hospital publishes the medical treatment resources (e.g., number of doctors, nurses, and hospital beds) of their emergency service center. The emergency service center advertisement must be updated in real time. When the patient requires a service, the agent activates an advertisement search, searching for a resource that is most advantageous to the patient. When searching for an appropriate hospital, the agent transmits the patient data and health history to the hospital. Thus, the hospital knows the patient's condition, enabling the quick preparation of equipment and medical treatment resources. In addition, the emergency service center can send an ambulance to the patient.

An advertisement system must immediately and accurately record medical resources, enabling the agent to select the correct hospital in real time. Emergency service centers and the hospital-advertisement content require the adoption of the time-to-live (TTL) method for updates. The TTL method can remove old messages in emergency service center advertisements. Advertisements have built-in validity times, and are automatically deleted when they exceed their time limits.

Figure 4 shows an MA based on the P2P network process:

(1) When the MA transport encrypts a document to be sent to the hospital platform, it creates a connection with the emergency service center, and the emergency service center is responsible for delivering the request to the hospital's platform in real time. First, the patient sends a request to the service center of an emergency service center.

Fig. 2 An example of announced advertisement

```
<?xml version= "1.0" encoding = "UTF-8" ?>
<!DOCTYPE jxta:PeerAdvertisement>

<jxta:PeerAdvertisement xmlns:jxta="http://jxta.org">

          <PId>
          urn:jxta:uuid-96162646162614A757874614D504725184FBC4E5D498AA0919F662E40028B04
          </PId>
          <GID>
          urn:jxta:jxta-HospitalGroup
          </GID>
          <Name>
          A-Hospital
          </Name>
          <Date>950611</Date>
          <Time>13:30</Time>
          <interventional surgery>cardiac catheterization</interventional surgery>

</jxta:PeerAdvertisement>
```

(2) The emergency service center features a helper agent for transactions that receive service requests and searches for announcements to locate an advantageous medical institution for the patient in the system. This mechanism considers various information including hospital beds and the patient's location.
(3) The TTL method enables emergency the service-center advertisements to receive accurate announcements in real time that are related to hospital records regarding hospital beds, nurses, and physicians.
(4) When searching for a hospital, the emergency service center sends information to the patient and the hospital to direct an ambulance to the patient's location.

When an MA receives the information, it transmits the patient's data and medical history to the hospital, enabling the hospital to rapidly assimilate the patient's condition. The MA currently performs well.

Secure mobile agent for telemedicine based on P2P networks

By binding usage restrictions to the signature key provided to an agent, we can potentially limit the damage from a malicious host. In this paper, rather than equipping an agent with a function, the patient produced (I, R), then I, R and

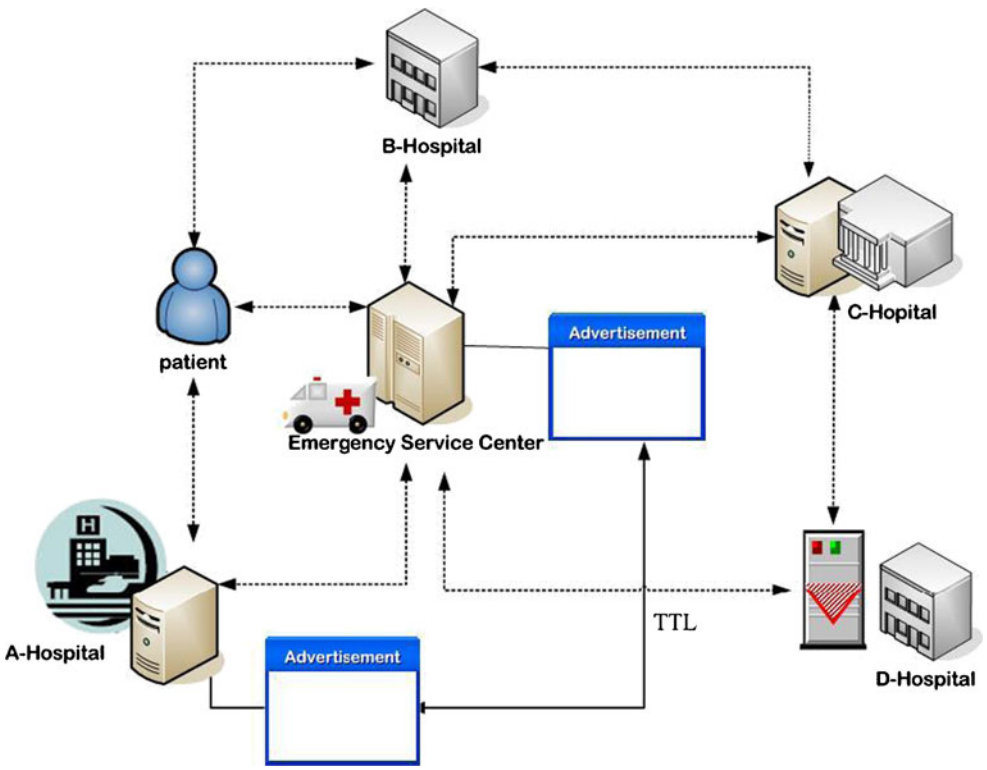

Fig. 3 An example of unpredictable telemedicine-service model base on P2 P network

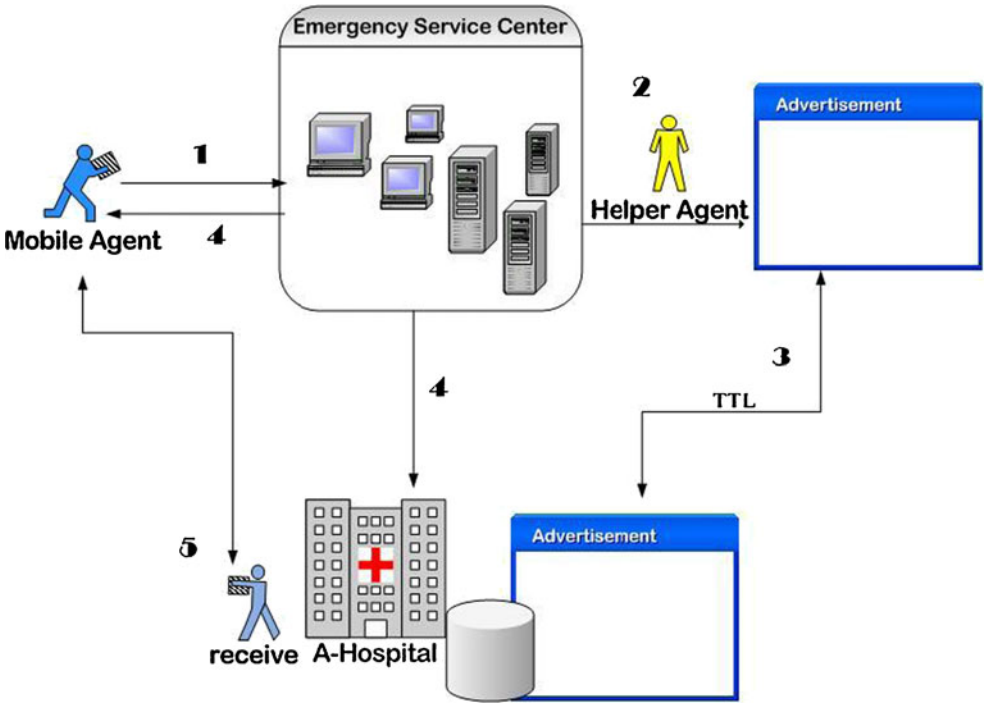

Fig. 4 Mobile agent system based on P2P Network architecture

(G, H), or the agent. Second, (G, H) read the agent's "undetachable signatures." If A has a transaction to sign, the agent platform must perform X = h(B), and the undetachable signature is (G^X, H^X). In addition, $G^X = (H^d)^X = H^{dX} = H^{Xd} = (H^X)^d$ and (I→Agent's ID, R→encrypted patient data and medical history) (Fig. 5).

During transportation, the exchange function is not conveyed to the hospital's platform but by the function encrypting the exchange to the hospital's platform. After receiving the encryption function from the patient's peer and deciphering the function, the hospital platform can obtain the patient's history. The hospital can obtain the patient status and prepare medical resources.

Thus, the proposed approach can effectively resolve and guarantee trust problems for action agents and agent platforms, guaranteeing the transported data of the two hospitals.

The emergency service center sends an ambulance to the patient's location while searching for an appropriate hospital. In the advertisement system, real-time and accurate records regarding the hospital's medical resources must be transmitted. This helps the patient obtain medical services. After decryption of the patient's data and medical history,

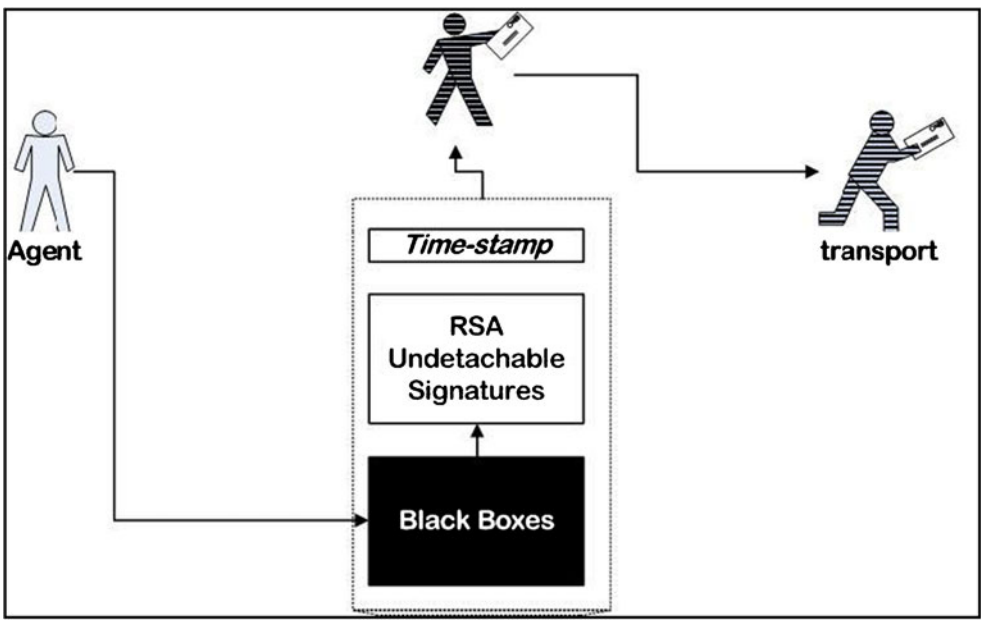

Fig. 5 Time-limited Black Boxes

the hospital understands the patient's condition. Thus, the hospital can quickly prepare medical resources.

Conclusion

The central challenges for telemedicine based on P2P networks include numerous new requirements and local variations in telemedicine service provisioning and medical practices. Four security requirements for telemedicine based on P2P networks are discussed in this paper: (a) confidentiality: patient privacy; (b) integrity: patient data security; (c) reliability: real-time; and (d) non-repudiation: medical information and service non-repudiation.

The proposed P2P network architecture, based on JXTA network platforms for telemedicine, implements two service model types: a predictable service model and an unpredictable service model. This architecture employs a two-layer safety mechanism for MAs (i.e., time-limited black boxes and RSA undetachable signature technologies), to provide a secure solution for agent-based telemedicine services. The proposed approach combined patient data, history, and a privacy key, making the data undetachable. On the other hand, MAs transmitted patient data to hospitals or emergency service centers using a secure transport. This helps patients obtain care in real time, reducing expenditures related to medical resources and personnel costs.

The future work of the proposed secured agent-based telemedicine architecture includes two directions. First, incorporate the proposed architecture with the role-based access control mechanism for accessing particular patient records. Next, according to the mobile devices are more and more popular today. Smart phone and tablet computer play an important role in modern telemedicine. The new security requirements of such application model should be discussed as well.

Acknowledgments This project was supported by the National Science Council of Taiwan (Grant No: NSC99-2221-E-320-005).

References

1. Norris, A. C., *Essentials of Telemedicine and Telecare*. Wiley Press, Chichester, 2002.
2. Charles, B. L., Telemedicine can lower costs and improve access. *Healthc. Financ. Manag.* 54(4), Oak Brook, Ill.: The Healthcare Financial Management Association, pp. 66–69, 2000.
3. Field, M. J. (Ed.), *Telemedicine: A Guide to Assessing Telecommunications in Health Care*. National Academy Press, Washington, D.C, p. 26, 1996.
4. Martin, E., *Military Healthcare Service System*. *Proceedings of the AFEC*, 1996.
5. Fakas, G. J., and Karakostas, B., A peer to peer architecture for dynamic workflow management. *Proc. Elsevier Inf. Softw. Technol.* 46:423–431, 2004.
6. Sameh, A., and Fakhry, D., Security in Mobile Agent Systems. Proceedings of the 2002 Symposium on Applications and the Internet (SAINT '02), pp. 4–5.
7. Reina-Tosina, J., Roa, L., and Rovayo, M., NEWBET: Telemedicine platform for burn patients. *IEEE Trans. Inf. Technol. Biomed.* 4(2):173–177, 2000.
8. Koutkias, V. G., Chouvarda, I., and Maglaveras, N., A multiagent system enhancing home-care health services for chronic disease management. *IEEE Trans. Inf. Technol. Biomed.* 9(4):528–537, 2005.
9. Pang, X., Catania, B., and Tan, K. L., *Securing Your Data in Agent-Based P2P Systems. Proceedings of the Eighth International Conference on Database System for Advanced Applications(DASFAA'03)*.
10. Li, T. Y., Zhao, Z. G., and You, S. Z., *A-Peer: An Agent Platform Integrating Peer-to-Peer Network. Proceedings of the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'03)*.
11. Hohl, F., Time limited black box security: Protecting mobile agents from malicious hosts. Lect. Notes Comput. Sci. 1419: 92-113, 1998.
12. Borselius N., Mobile agent security. *Electron. Commun. Eng. J.* 14(5):211–218, 2002.
13. Davidson, A., *P2P File Sharing Privacy and Security, Testimony before the House Committee on Government Reform Center for Democracy and Technology*, May 2003.
14. Balfe, S., Lakhani, A. D., and Paterson, K. G., *Trusted computing: providing security for peer-to-peer networks*. *Proceedings of the 15th IEEE International Conference Peer-to-Peer Computing*, Aug.-2 Sept. 2005, pp. 117–124.
15. Sander, T., and Tschudin, C. F., *Protecting mobile agents against malicious hosts. Proceeding of Mobile Agents and Security*, 1998, pp. 44–60.
16. Aberer, K., Datta, A., and Hauswirth, M., Efficient, self-contained handling of identity in peer-to-peer systems. *IEEE Trans. Knowl. Data Eng.* 16(7):858–869, 2004.
17. Mea, V. D., Agents acting and moving in healthcare scenario—a paradigm for telemedical collaboration. *IEEE Trans. Inf. Technol. Biomed.* 5(1):10–13, 2001.
18. Chen, R. Y., and Yeager, B., *Java Mobile Agents on Project JXTA Peer-to-Peer Platform. Proceedings of the 36th Hawaii International Conference on System Sciences(HICSS'03)*, 2003.
19. Kotzanikolaou, P., Burnester, M., and Chrissikopoulos, V., Secure transactions with mobile agents in hostile environments. *Lect. Notes Comput. Sci.* 1841:289–297, 2000.
20. Ng, W. S., Ooi, B. C., Tan, K. L., and Zhou, A., *PeerDB: A P2P-Based System for Distributed Data Sharing. Proceedings of the 19th International Conference Data Engineering*, pp. 633–644, March 2003.
21. Li, Z., Dong, Y., Zhuang, L., and Huang, J., *Implementation of Secure Peer Group in Peer-to-Peer Network. Proceedings of ICCT2003*, 2003.
22. Yu,C. R., and Bill, Y., *Java Mobile Agents on Project JXTA Peer-to-Peer Platform. Proceedings of the 36th Hawaii International Conference on System Sciences(HICSS'03)*.
23. William, Y., and Williams, J., *Secure Peer-to-Peer Networking: The JXTA Example, Proceedings*. 2002 IEEE 1520-9202, March | April 2002, pp. 53–57.
24. Pank, Z. W., Lee, J. H., and Kim, M. K., *Design of Security Functionality in P2P Applications. Proceedings of the 8th Russian-Korean International Symposium, Science and Technology*, Vol. 1, 26 June-3 July 2004, pp. 132–136.