

JXTA ネットワークに対するユーザ認証およびアクセス制御の導入

TRAN XUANHOA †, 杉原 健司 †, 吉永 努 †, 曾和 将容 †

あらまし P2P 技術は様々なデバイスを対等な立場で接続し、直接情報のやりとりを行うネットワーク形態として最近注目されている。この技術により、ネットワーク上にある様々なサービスを容易に提供することができる。しかし、セキュリティの確保や安全なバーチャルグループの提供などは課題となっている。本論文ではその課題を解決するために、P2P の JXTA ネットワークにおいて安全で信頼できるマネジメントピアを実装し、ユーザ認証およびアクセス制御メカニズムを提案する。

Introduction of User Authentication and Access Control Mechanism into JXTA Network

XUANHOA TRAN †, KENJI SUGIHARA †,
TSUTOMU YOSHINAGA † and MASAHIRO SOWA †

Abstract JXTA is a set of open, generalized Peer-to-Peer (P2P) protocol that allows any connected devices on the network to communicate and collaborate as peers. This paper presents a mechanism for user authentication and access control in the JXTA network and its implementation. We introduce a management mechanism that allows clients and service providers to connect and communicate securely by accessing to a management peer. Clients can join a secured virtual group from which they can download trusted services.

1. Introduction

Peer-to-Peer (P2P) networks are becoming increasingly popular because they provide opportunities for real-time communication, ad-hoc collaboration and information sharing in a large-scale distributed environment [1].

P2P communication software is being used to allow individual hosts to anonymously share and distribute various types of information over the Internet. While systems based on central indices such as Napster [2] collapsed due to litigations over potential copyright infringement, the success of pure P2P products like Gnutella [3] and Freenet [4] fostered interest in defining a global P2P infrastructure for information sharing and distribution. On a P2P network, member peers have flexible roles

and may function at the same time as clients and servers. Most P2P systems protect peers anonymity, allowing them to use self-appointed opaque identifiers when they advertise shared resources, such as music files or video clips.

Sun has developed JXTA technology [5] that creates a common P2P platform. This platform makes it simple and easy to build a wide range of distributed services and applications. It enables developers to focus on their own application development; making distributed computing software flexible, interoperable, and available on any peer on expanded Web.

Security in the P2P network is one of the most important themes [6][7]. JXTA technology provides a mechanism of inexpensive CA (Certification Authorities) in each peer to authenticate other peers and access to a peer group in which clients can

† 電気通信大学大学院情報システム学研究科
The Graduate School of Information Systems,
University of Electro-Communications

communicate with each other. But it is not easy to manage members in the group or to allow a specific peer who has sufficient permission to access the service, which is provided by the peer. VHE (Virtual Home Environment) Certificate Manager Service manages authentication for the individual connection [6]. The peers, which received a signed certificate, have permission to access to all other peers within a home network [8]. Ohya et al. suggest a mechanism that uses IC card to build the trusted domain (or group) for a cooperative work, and the client needs the IC card every time to join the domain [7]. However, the above technologies seem not flexible enough if we want tighter control of the group. We need a mechanism that provides a secured virtual group in which we can provide service to the clients. There are some problems in controlling the group, which clients and service providers belong to. A centralized manager seems to be needed to provide a secured virtual environment in the P2P network.

In this paper, we present a mechanism of user authentication and access control in the JXTA network. In this mechanism, member peers can check other peers by requesting a trusted management peer and get a trusted service. This management peer acts as a centralized look-up server to manage users and services. In addition, the management peer authenticates clients and service providers. Then it establishes secured communication between clients and service providers.

2. JXTA network

2.1 Overview

JXTA network is a virtual network on top of the existing physical network infrastructure where services and applications are built. This network layer is thin and simple, but provides interesting and powerful primitives for services and applications [5]. The main purpose is to hide all of the complexity of the physical network topology (firewall and NAT, etc.), and providing a uniform addressable

network for all peers in the network. This network allows a peer to exchange messages with any other peers regardless of its network location. Messages are transparently routed, potentially traversing firewalls or NATs, and being able to use different transport/transfer protocols (TCP/IP, HTTP) to reach the receiving peers. This network standardizes the manner in which peers discover each other, self-organize into peer groups, advertise and discover network resources, communicate with and monitor each other.

2.2 Security in JXTA

(1) Private connection

Peers in the JXTA network are connected and they can exchange messages through pipes. Multiple pipes between two peers always share a single TLS (Transport Layer Security) connection. Within that connection, a public key is also shared over multiple pipes and all messages will be encrypted before transferring through the pipes.

(2) Authorization

JXTA provides an entry-level trust model, which costs nothing and is appropriate for content sharing, secure financial transactions, and so forth. Poblano [9], a JXTA trust model, permits peers to be their own certificate authorities, or socially accumulating inter-peer interactions. At the same time, peers may form peer groups where a member may be designated as a CA for that group, with its root certificate as part of that peer group's binary.

3. Peers and their connections

When an internet-connected device (PCs, mobile, etc.) joins to a JXTA network, it may become a service provider or a client. A service provider permits specified peers to use its service while a client utilizes the service that is provided by the trusted service provider.

In this mechanism, we suggest that the service provider offers a private service such as file service in an office or a service that

controls devices in a home network. Clients can download these services by using PC or mobile devices. The service provider has to identify the client precisely who is trying to access the service. We have designed both the service provider and the client, which should be managed by a trusted management peer that is called MP (Management Peer).

The design of user authentication and access control mechanism is shown in Figure 1. In this mechanism, we have three kinds of peer: MP, client, and service provider peers. At first, a client and a service provider connect to the MP through a public bi-pipe (bi-directional pipe). After the connection is established, the MP creates two private bi-pipes, one is for the client and other is for the provider, so that the communication between the MP with the client or the service provider is secure and private. Then a private bi-pipe connecting the client and the service provider is established. Finally, the service provider offers the service to the client through this bi-pipe.

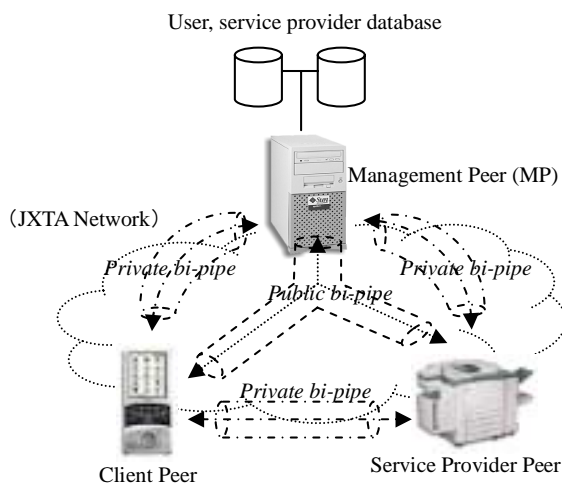


Figure 1: Connection among peers.

The description of the bi-pipes and the peers is below.

(1) Public bi-pipe:

This bi-pipe is created in MP to wait for the connection from clients and service providers.

Clients and providers must have the advertisement of this bi-pipe locally before connecting to the MP.

(2) Private bi-pipes:

There are three private bi-pipes in our mechanism: (a) MP-Client bi-pipe that connects a MP and a client, (b) MP-Provider bi-pipe that connects a MP and a service provider and (c) Provider-Client bi-pipe that connects a client and a service provider.

The first two bi-pipes are created in a MP. Their advertisements are transferred to a client or a provider after successful authentication. The last one is created in a service provider and its advertisement is transferred to the client after successful authorization.

(3) Management Peer (MP)

MP manages a user and service provider database that contains the user accounts and access information for services. This peer acts as an access point, similar to a rendezvous peer, then controls access between clients and service providers (role of look-up server). The MP waits for the connection requests from clients and service providers on the public bi-pipe and accepts the connection coming from clients and service providers.

(4) Service provider peer

This peer connects directly to the MP through a MP-Provider bi-pipe. It must register a name and an advertisement of a Provider-Client bi-pipe for each of its service to the MP. After the registration process, it binds to the Provider-Client bi-pipe to wait connection from clients. When a connection is requested, it will ask the MP to authorize the client and will provide its service to the client if the authorization succeeds.

(5) Client peer

Client peer connects directly to the MP to request a certificate via a MP-Client bi-pipe. After obtaining a list of service from the

certificate, the client selects a service and communicates with the service provider through the Provider-Client bi-pipe, which is created by the provider.

4. Implementation

We divide the implementation into five processes listed below (Figure 2).

- (1) Confirming the MP.
- (2) Getting a certificate.
- (3) Registering a service.
- (4) Requesting a service.
- (5) Downloading a service.

Subsections 4.1 to 4.5 describe these processes in detail.

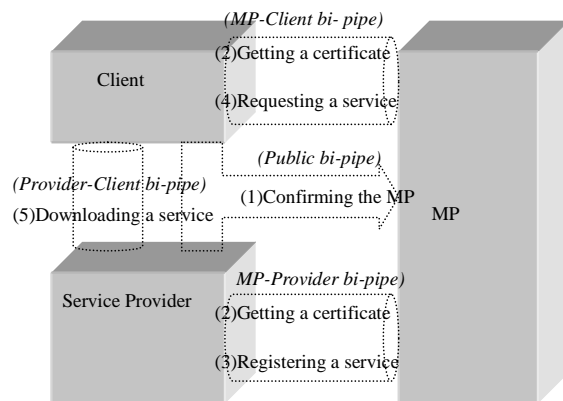


Figure 2: User authentication and access control mechanism.

4.1 Confirming the MP

When clients or service providers connect to a specified MP through the public bi-pipe, they should be certain that this peer is the trusted MP before they begin the process. The trusted MP knows exactly the account of clients or the service providers. Authentication process of a trusted MP is described as the following.

Step 1: Client (or service provider) sends its own ID.

Step 2: When the MP receives an ID, it checks the existence of this ID in database. If this account exists, the MP creates a communication key and a MP-Client (or a MP-Provider) bi-pipe for communicating with

this peer.

Step 3: the MP encrypts the communication key, the ID, and the bi-pipe advertisement by using the password for this ID, and then sends this data to the peer.

Step 4: when the peer received the message from the MP, it decrypts the message by using its own password. If the encrypted ID is same with its own ID, the MP is confirmed successfully.

4.2 Getting a certificate

After confirming MP, a client (or a service provider) uses the MP-Client (or MP-Provider) bi-pipe to connect and sends its own password to the MP. Messages will be encrypted using the communication key before being exchanged. The MP receives the message including ID and password, and then issues a certificate after the authenticating process. The certificate of the clients includes data listed below.

- (1) ID: the ID of the client.
- (2) Begin Time: the time this certificate is issued.
- (3) TTL (Time-To-Live): the valid period for this certificate. This value is 2 hours.
- (4) Service list: a list of the services that the client can use

The certificate of the service provider includes only the ID and the Begin Time entries. The provider stays valid through out a given period of time.

4.3 Registering a service

If a service provider receives a valid certificate from the MP, it registers its service name with an advertisement of a Provider-Client bi-pipe to the MP. The MP adds this information to an available service list. By using a setting tool, we can put this service to a group of users so that a client in this group has permission to utilize the service.

The MP checks the continuous existence of the service provider by sending a LOOKUP message periodically. When the provider

receives this message, it replies a CONFIRM message. The MP will remove the service from the valid service list when it does not receive a reply from the service provider.

4.4 Requesting a service

A client must get an advertisement of a Provider-Client bi-pipe in order to connect to a service provider. After receiving a valid certificate from the MP, the client can obtain a list of service from it. Then, the client selects a service from the list and sends a bi-pipe advertisement request together with its certificate to the MP. The MP authorizes the certificate and replies with the advertisement of Provider-Client bi-pipe to the client.

4.5 Downloading a service

After getting the advertisement of Provider-Client bi-pipe, the client uses this advertisement to bind to the provider. Then the client sends a download service request together with its certificate to the provider via the Provider-Client bi-pipe. Next, the provider requests the MP to authorize the client. Finally, the provider sends out the requested service to the client after the authorization succeeds.

5. Experiments and Considerations

5.1 Experiments

In order to evaluate the proposed mechanism, we developed three applications, which are executed on the MP, the client peer and the service provider. The following issues are significant points to be evaluated.

- (1) Client and service provider must confirm the trusted MP.
- (2) The MP, being a trusted manager, authenticates client and service provider through a secured bi-pipe.
- (3) The client and the service provider, which are authenticated successfully, can communicate using a Provider-Client bi-pipe, and the client will be authorized each time it sends a request to the service provider.
- (4) The private bi-pipes, which are established,

are secure. Other peer cannot crack the data being transferred via these pipes.

A private network environment is used for the experiment of the mechanism. An encrypting algorithm uses 8 bits (which can be easily upgraded to 128 bits) block cipher, which is provided in JDK 1.4, java.security, and javax.crypto packages. We implemented a service called a Calculation service which provides a simple calculation. Client downloads this service (class file) and can execute it on the client peer.

Figure 3 displays the client peer application. User inputs its ID and a password and then retrieves a list of services including the Calculation service. This list is shown on a service list box. User selects a service and downloads it by clicking the Download service button.

5.2 Considerations

We confirm the security aspects of the proposed mechanism.

(1) Avoiding masquerade by a malicious MP

In this mechanism, the client confirms the identity of the MP by checking whether the MP knows the exact password of the client. If the password is correct, the client can decrypt the message.

(2) Preventing unauthorized access by a client

Only after the client is correctly authenticated and authorized by the MP, it can establish the private bi-pipe using the advertisement from the MP.

(3) Preventing unauthorized access by a malicious service provider

Service providers are authenticated by the MP so that the registration of a service from a failed provider is impossible.

(4) Avoiding a security hole posed by the downloaded service

The downloaded service will remain on the client. However, if the client tries to send a command to the service provider through that service, it has to go through the authorization process again.

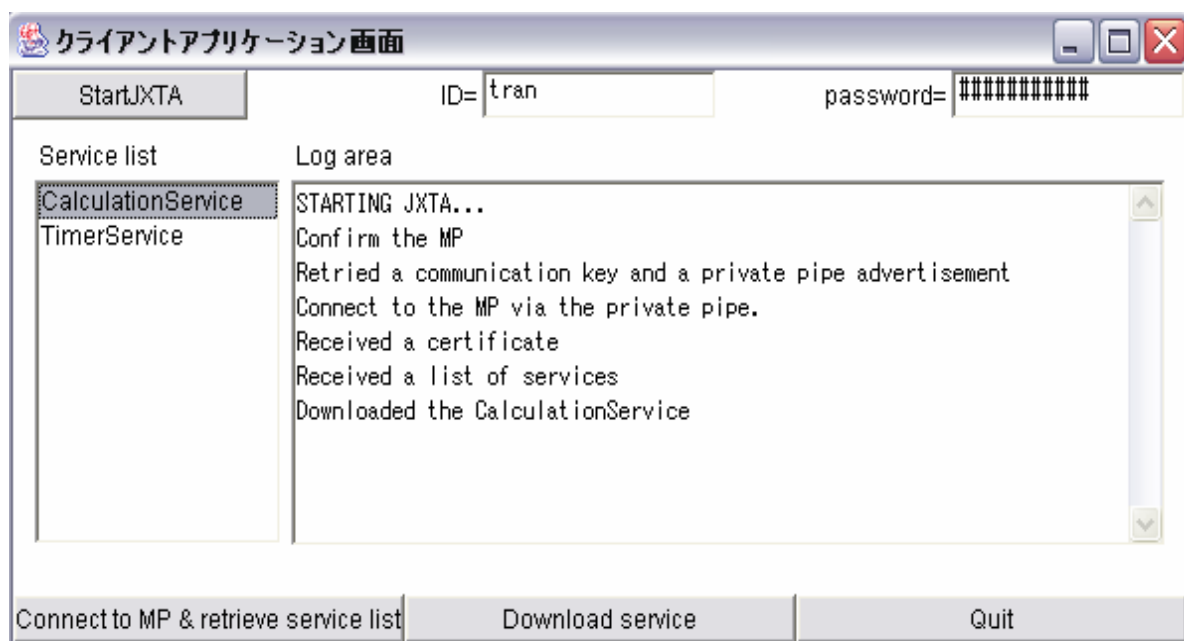


Figure 3: An example of client application.

6. Conclusion and Future Work

In this paper, we have discussed a new mechanism of authenticating user and access control in the JXTA platform. By using this mechanism, trusted clients can easily access to trusted service providers. The communication between the client and the service provider is secure through the private bi-pipe, which is created by the service provider. Furthermore, all the data, which are transferred through the private pipe, is encrypted so that other peer cannot crack. We described the first step toward a secure mechanism of user authentication and access control in the P2P network.

So far, we have implemented the MP as a rendezvous for clients and service providers. We should implement more simultaneous MPs so that when one is down, clients and service providers can access to another.

We also need to complete an application for the MP in order to manage accounts of clients and service providers more easily.

References

- [1] D.S.Milojicic, V.Kalogeraki, and editors. Peer-to-Peer Computing, Hewlett-Packard, March 2002.
- [2] Napster. <http://www.napster.com>.
- [3] Gnutella. <http://www.gnutella.com>.
- [4] Freenet. <http://freenetproject.org>.
- [5] Sun Microsystems. Project JXTA. <http://www.jxta.org>.
- [6] C.Loeser, W.Mueller, F.Berger, H.J.Eikerling. Peer-to-Peer Networks for Virtual Home Environments. 36th Annual Hawaii International Conference on System Sciences, January 2003.
- [7] H.Ohya, R.Miyaji, Y.Sugawara, and K.Okada. A Proposal for P2P-based Communication Platform Using IC Card. Journal of Information Processing Society of Japan, Vol. 44, No. 8, pp.2051-2059, 2003.
- [8] E.Turcan, R.L.Graham. Peering the Smart Homes. Proceedings of the First International Conference on Peer-to-Peer Computing, 2002.
- [9] R.Chen and W.Yeager. Poblano-a distributed trust model for peer-to-peer networks. JXTA Security Project White Paper, 2001.