Proceedings of the IASTED International Conference
COMMUNICATION SYSTEMS AND NETWORKS
September 1-3, 2004, Marbella, Spain

A PROPOSAL OF USER AUTHENTICATION AND A CONTENT DISTRIBUTION MECHANISM USING P2P CONNECTION OVER A MOBILE AD HOC NETWORK

Masato Oguchi, Yoshiko Nakatsuka†, and Chiho Tomizawa‡
Department of Information Sciences, Ochanomizu University
2-1-1 Otsuka Bunkyo-ku, Tokyo, 112-8610 Japan
email: oguchi@computer.org

ABSTRACT

Recently, content distribution services over a network have been expanded to a mobile environment. However, as the volume of data increases and higher quality of services is demanded, a throughput restriction over wireless communications has become a bottleneck. In order to compensate the low bit-rate cellular line, a peer-to-peer (P2P) connection over a mobile ad hoc network is applied. High throughput communications are available on the ad hoc network using broadband wireless LAN.

In order to realize a content distribution service on the mobile ad hoc network, a user authentication mechanism is indispensable. Because a server for user authentication is not always available on the ad hoc network, an idea of multistage classified groups based on a temporary identification is proposed. Moreover, since the ad hoc network is not always connected, a high-functional client that redistributes content is introduced for realization of the content distribution service.

The proposed ideas are implemented on an experimental system using JXTA, an all-purpose P2P platform. According to the result of experiments, the user authentication and content distribution mechanisms work well on the P2P connection over the mobile ad hoc network.

KEY WORDS

Mobile Ad hoc Network, Peer-to-Peer, User Authentication, Content Distribution, Wireless IP Networks, Mobile Computing

1 Introduction

As performance of mobile terminals has improved, a content distribution service that provides a mass of data to users is desired on mobile communications. In such services, using only a cellular network is not sufficient in terms of its bandwidth and costs. Broadband wireless LAN is expected to remedy the cellular networks[1]. However, fixed hot-spots cannot cover a wide area by themselves. Thus, an ad hoc networks using broadband wireless LAN is drawing much attention, in which users are connected directly as a peer-to-peer (P2P) manner, independent of a particular hot-spot. P2P is expected to exploit distributed computer resources and share contents efficiently[2][3][4].

An ad hoc network on mobile communications is a form of multiple nodes' connection, in which each mobile node connects with adjacent one when it goes out, and there is no management server on the network. Therefore, only limited services are available on contrast to the case of connecting to an infra-network. In this case, developing a framework of using an ad hoc network for content distribution services is meaningful, because wireless LAN provides much wider bandwidth compared to a cellular line. For the realization of content distribution services, a user authentication method is indispensable. This is a basic mechanism to decide which user is allowed to have a right to take which services, without connecting to an infra-network. Authentication is also essential to protect from malicious users and devices.

In this paper, a framework of user authentication on an ad hoc network is proposed. In this idea, authentication levels are given to multistage groups, and a user joins to an appropriate group depending on its authentication level, so that a particular service is available which is provided to the member of the group. A method of content distribution services on an ad hoc network is also studied, in which a rich client model is introduced. The proposed ideas are implemented using JXTA, an all-purpose P2P platform.

The rest of the paper is organized as follows. A user authentication mechanism is proposed in Sec.2. It is implemented using JXTA on an experimental system, and its behavior is verified in this section. In Sec.3, a content distribution framework on an ad hoc network is discussed. It uses a broadband P2P connection over a mobile ad hoc network. Final remarks are made in Sec.4.

†Currently with Nihon Unisys, Ltd.
‡Currently with NEC Corporation

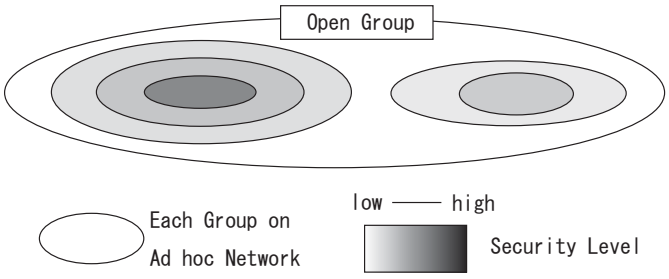

Figure 1. Multistage authentication group

2 User Authentication on a Mobile Ad hoc Network

2.1 A Proposal of a Multistage User Authentication Mechanism

In a mobile ad hoc network, since each terminal is not always connecting to an infra-network, it is difficult to reach a particular server. Therefore, it is impossible to realize complete authentication using a database on the server in the ad hoc network. However, the user's authentication level should be different from case by case, rather than all of them are identified as "unauthenticated". For example, a user with no acquaintance should be treated differently from a friend staying nearby, even on the same ad hoc network. From a viewpoint of service providing, users who have a right to receive the service and those who have no right should be classified differently.

In this paper, a multistage user authentication mechanism is proposed for a mobile ad hoc network. In this model, authentication levels are given to multistage groups. That is to say, a group contains a higher group inside it, and the higher group contains a much higher group. A user joins one of these groups based on its authentication level, and it will move to a higher group when its level is raised. This is illustrated in Fig.1.

An ad hoc network is open in most cases, so users can join to and remove from the network freely. A user belongs to an open group, which is not authenticated at all, when it joins to the network at first. Only limited services are available in this group. After a certain process, when the user's credit becomes higher, it moves to a higher authenticated group, and more services are available in it. For example, contents are provided depending on the group level of authentication.

A discussion how to change users' authentication level is beyond this paper. A simple example is to decide based on a certification held by users, and/or to change its authentication level when it is connected to an infra-network temporarily and admitted by a server. The authentication level is valid while a user stays in the ad hoc network. Each group is allowed to decide what types of service can be provided to its members.

2.2 JXTA

As an experimental platform to implement the proposed idea, JXTA is used. JXTA is a P2P platform developed by Sun Microsystems Inc., which is neither dependent on a language nor a computer system[5][6][7]. JXTA consists of a suite of protocols that produce a P2P application. It includes Peer Discovery Protocol (PDP), Peer Resolve Protocol (PRP), Peer Information Protocol (PIP), and so on. These protocols provide basic functions to generate and operate a P2P application, such as searching JXTA resources, defining query formats, and transferring information of each node.

By using JXTA, an application programmer can develop P2P software, paying little attention to detailed specifications. Because of its simplicity, JXTA can be deployed to many mobile devices that have a processing function such as PDAs and cellular phones, to provide the P2P solution to them. A basic unit of P2P processing on a P2P network is called a "peer" in JXTA. All peers do not have to implement all protocols. They can select protocols to implement, depending on the ability and their way to use. The peers are independent from each other and work asynchronously, but some peers make a group voluntarily based on a common interest. This is called a "peer group".

Both a peer and a peer group provide a service. The peer service is not available if the peer is not active. On the other hand, the peer group service has higher usability, because the service may be provided by another peer in the group, even if the original peer is not active.

2.3 Membership Service in JXTA

Although JXTA is a language-neutral framework, a programmer can employ "JXTA Java binding", a reference implementation developed using the programming language Java. In JXTA Java binding, basic P2P services are defined and their implementation is provided, based on the JXTA protocols. The defined Java interfaces are included in "net.jxta" package, and the implemented classes of the interfaces are included in "net.jxta.imple" package.

JXTA Java binding provides a membership service, administrating which peers join which peer groups. This is defined as a membership policy. As a reference implementation of the membership service, the following two services are prepared: One is "NullMembershipService", which only assigns identification and performs no authentication, and the other is "PasswdMembershipService", which has a simple authentication mechanism based on a login ID and an encoded password. However, this membership service is not sufficient as an authentication mechanism. In order to achieve practical authentication, a method of implementation must be defined for PasswdMembershipService, and information of account authentication should be generated and verified. In this paper, an authentication mechanism is implemented, in which multistage peer groups based on PasswdMembershipService is

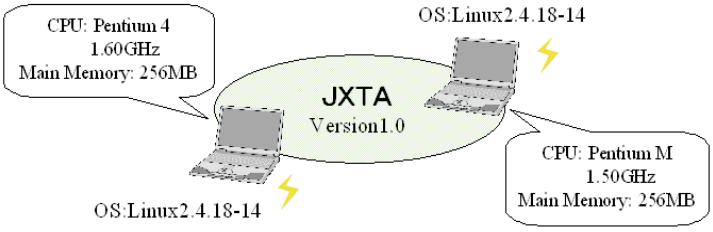

Figure 2. Environment of the experimental system

realized.

2.4 Implementation of Proposed Authentication Mechanism

The proposed multistage authentication mechanism is implemented on a mobile ad hoc network using JXTA. As an operating system of the experimental system, Linux2.4 is used as shown in Fig.2. Two notebook PCs are connected with an ad hoc network using IEEE802.11b wireless LAN, on which JXTA version1.0 is installed.

In order to create a peer group, a peer group advertisement is required. An advertisement is information described with XML documents, which indicates JXTA network resources like peer and peer group. In the peer group advertisement, basic information is shown such as a name of the peer group, its ID, explanation, and specification. All peers belong to a peer group called ”Net Peer Group”, and all groups are generated based on this group.

The following methods are defined in this experiment.

- CreateGroup()
  A module implementation advertisement that includes information about specification of Net Peer Group is copied, and a new advertisement is created and published. A new peer group is created based on the published peer group advertisement.

- CreatePeerGroup()
  For creating a secure peer group, PasswdMembershipService is used instead of the standard NullMembershipService. First, a module implementation advertisement based on PasswdMembershipService is created and published. Next, the module implementation advertisement, a peer group name, a login name, and a password are set to a new peer group advertisement to reflect a new membership service. The new peer group that supports authentication is created using the login ID and the password.

In the process of creating multistage peer groups, the CreateGroup() method is invoked at first, and an open group (called ”OrangePeerGroup”, for example) is created. Next, the CreatePeerGroup() method is called, and a secure peer group (called ”BluePeerGroup”) is created inside

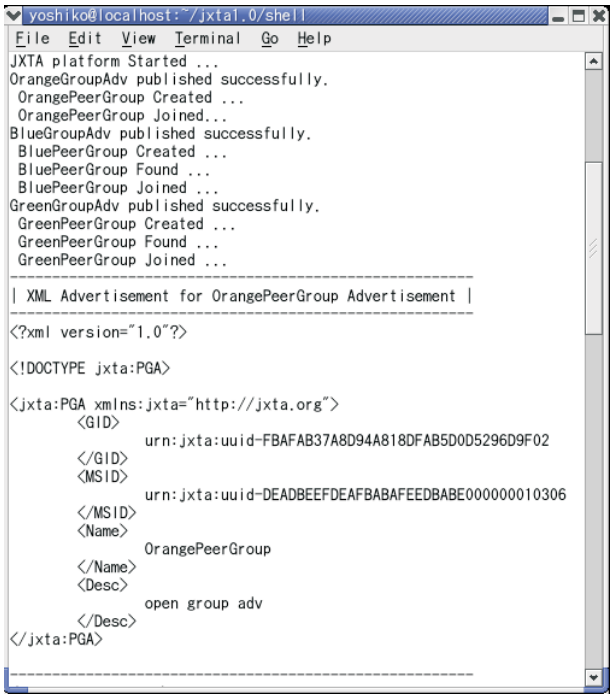

Figure 3. Creating secure peer groups on JXTA

the group using OrangePeerGroup as a parent peer group. In addition, another secure peer group (called ”GreenPeerGroup”) is created using BluePeerGroup as a parent, so that multistage authenticated peer groups are generated. The execution of the creating these groups is shown in Fig.3.

Another peer can join to the created peer groups using JXTA Shell, one of useful JXTA applications. This execution is shown in Fig.4.

In JXTA Shell, after a peer group discovery message is sent using ”groups -r” command [①], a group list is shown using ”groups” command [②]. ”join -d group0” command is issued to join OrangePeerGroup, one of the discovered groups [③]. Because OrangePeerGroup is an open group, a user can join it only with its ID. This is verified with ”join” command [④]. Next, peer groups in the OrangePeerGroup is found using ”groups -r” and ”groups” commands [⑤][⑥], ”join -d group0” is executed to join BluePeerGroup. Because BluePeerGroup is a secure group that requires authentication, a user can join it only with correct ID and password. Thus, the proposed multistage secure peer groups are realized on the experimental environment.

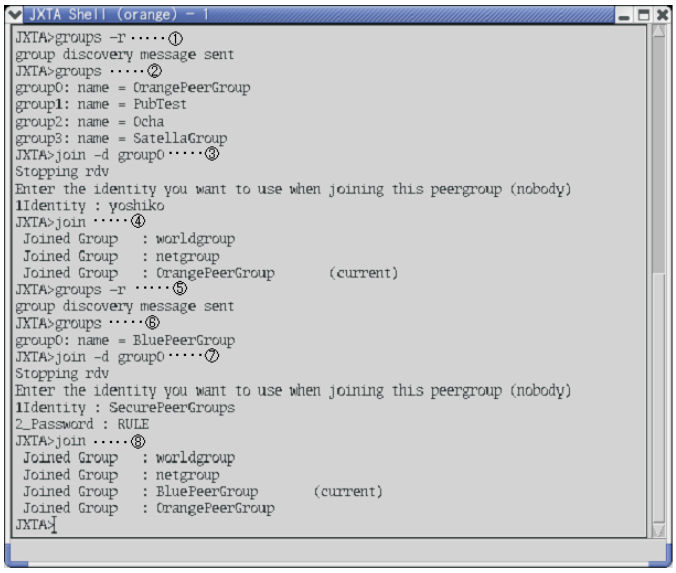

Figure 4. Join to an authentication group using JXTA Shell

3 Content Distribution Service using P2P Connection

3.1 A Rich Client Model

In mobile communications, a client terminal only has a display function like a browser, and a server on the network execute most of jobs. Currently, such a thin client model is a mainstream in the web-based services[8]. However, the components for mobile computing have become powerful recently[9]. A rich client, huge volume of data can be stored and processed on it, is coming to be available.

In this model, for example, contents are downloaded and stored at the client while it is connected to an infra-network, so that user can make use of the data even in an offline case. Moreover, as contents can be redistributed among clients using a broadband P2P connection, availability of service increases on a mobile ad hoc network. Different from wired connection cases, it is hard to expect broadband always-on communications in mobile communications. In this paper, a content distribution service is discussed based on such a rich client model on the ad hoc network. An overview of this idea is shown in Fig.5.

An efficient content distribution is expected on the client, using not only a direct connection with a content provider but also a broadband P2P connection on the ad hoc network. Furthermore, an original content produced by the client can also be provided. A method to arrange the position of cached contents is studied in literatures[10][11]. In our research work, the ad hoc network part in Fig.5 is prepared, and a client-server type content distribution mechanism is implemented using the P2P connection.

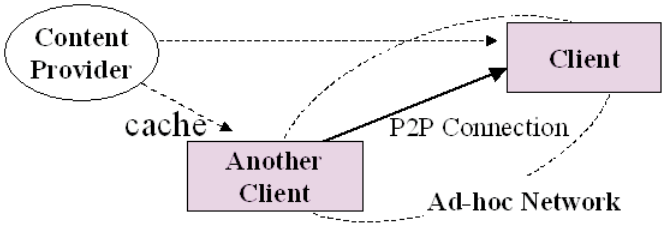

Figure 5. Content distribution service on an ad hoc network

3.2 Pipe Service in JXTA

Pipe Binding Protocol (PBP) is one of the basic JXTA protocols, and a pipe service is realized based on this protocol. A pipe is an abstract object that is defined as a connection between endpoints. A connection can be built from one source endpoint to one or more destination endpoints. A unicast pipe is a connection to a single pipe, and a propagate pipe bind to multiple pipes. A user can decide which type of pipes is used, when a pipe advertisement is created. In this paper, a mechanism of content distribution services on the ad hoc network is realized using the pipe service in JXTA.

3.3 Implementation of Content Distribution Service

3.3.1 Message Transfer

A message transfer program is developed using JXTA services, in which peers can send a message to other peers. In the program, a client discovers a group that is created and published by a server to provide a service. The client retrieves pipe information from the discovered service advertisement, creates its own pipe based on the information, and connects to the group through the pipe. A message is transferred through a common message tag. The sender sets the message to the tag as String data, and the receiver retrieves and displays it.

According to this procedure, a message transfer connection is established between groups. Using the program, the server displays its contents to the client, who can request what it wants based on the information.

3.3.2 Content Distribution

The message transfer program explained in the previous subsection is extended to cope with contents. In this paper, contents stand for images, voices, and executable binary data. Because binary data doesn't have a boundary of character code, it cannot be processed as String data like a message. Thus, the server sets the data to a tag as a byte

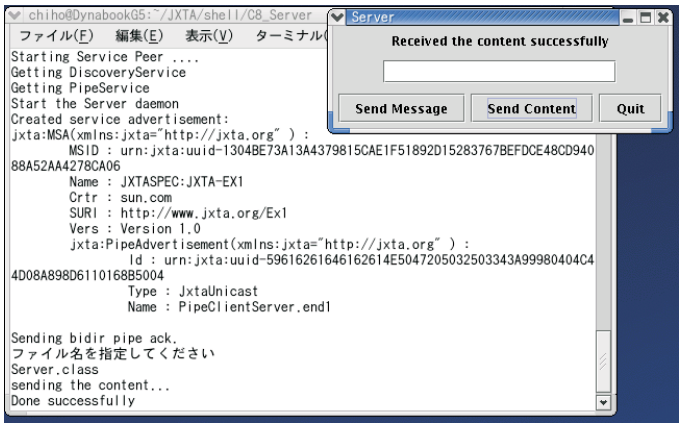

Figure 6. Execution on server side

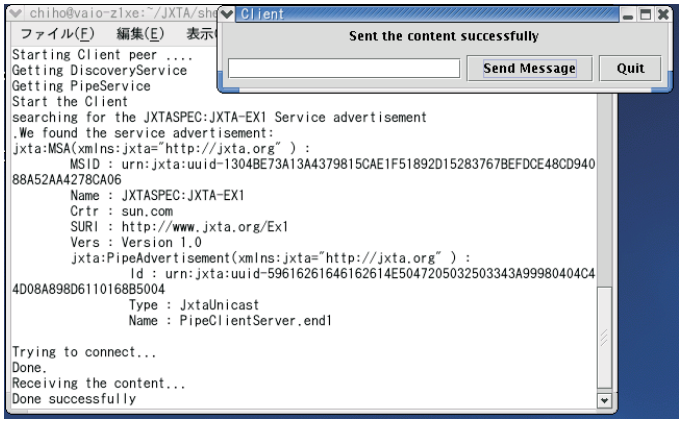

Figure 7. Execution on client side

type structure within a designated size, and transfers it repeatedly until the end of the data. The client retrieves the byte type structure from the tag, and writes it to a file.

The execution of the content distribution program is shown as follows. First, a user interface appears on both the server and the client sides, when the program begins. On the server side [Fig.6], ”Send Message”, ”Send Content”, and ”Quit” buttons are provided. ”Send Message” and ”Quit” buttons can be used on the client side [Fig.7]. When a message is given to the user interface frame and the ”Send Message” button is pushed, the message appears on the user interface frame on the counterpart. The server can give content to the client based on a request of the content. The client will receive the content and store it automatically only by the request to the server. In the example of the figures, the server sends its executable file ”Server.class” to the client, and the client receives it and executed properly.

4 Conclusion

An ad hoc network, a temporary network connected with neighbor nodes, is expected as a platform of services in which mass data is transferred and processed. For such a purpose, a user authentication mechanism is essential. Thus, an authentication framework based on multistage groups is proposed, and implemented using JXTA in this paper. In order to realize a content distribution service in a mobile ad hoc network, a rich client model is introduced. This is also implemented using JXTA. According to the result of the execution, the proposed ideas work well on the P2P connection over the mobile ad hoc network.

As a future work, we will discuss how to execute authentication of each user on the mobile ad hoc network, and how to change the authentication level on each case actually.

References

[1] J. Ala-Laurila et al., ”Wireless LAN Access Network Architecture for Mobile Operators” IEEE Communications Magazine, vol.39, no.11, pp.82-89, November 2001.

[2] H. Balakrishnan, ”Looking Up Data in P2P Systems” Communications of the ACM, vol.46, no.2, pp.43-48, February 2003.

[3] M. Milenkovic et al., ”Toward Internet Ditributed Computing” IEEE Computer, vol.36, no.5, pp.38-46, May 2003.

[4] A. W. Loo, ”The Future of Peer-to-Peer Computing” Communications of the ACM, vol.46, no.9, pp.56-61, September 2003.

[5] Project JXTA, http://www.jxta.org/

[6] Projects::JXTA Book, http://www.brendonwilson.com/projects/jxta/

[7] J. D. Gradecki, Mastering JXTA, Wiley Publishing, Inc.

[8] I. Ahmad, ”Network Computers: The Changing Face of Computing” IEEE Concurrency, vol.8, no.4, pp.9-11, 2000.

[9] D. Clark, ”Mobile Processors Begin to Grow Up” IEEE Computer, vol.35, no.3, pp.22-25, March 2002.

[10] T. Hara, ”Replica Allocation for Improving Data Availability in Ad Hoc Networks” Transactions of the Institute of Electronics, Information and Communication Engineers, vol.J84-B, no.3, pp.632-642, March 2001.

[11] G. Cao et al., ”Cooperative Cache-Based Data Access in Ad Hoc Networks” IEEE Computer, vol.37, no.2, pp.32-39, February 2004.