5A−05

JavaCardを用いたピア・ツー・ピアによる動的なグループ構成法の提案

宮地 玲奈，小宅 宏明，菅原 陽子，岡田 謙一*
慶應義塾大学理工学部†

1　はじめに

近年，常時接続環境の整備に伴い，また，個人で使用する端末の能力は急速に向上し，以前サーバ・クライアント方式でサーバとしての役割を担っていたマシンと同等あるいはそれ以上の機能を持つまでになった．

このような背景や，著作権問題でも話題となった音楽ファイル交換サービスであるNapstarの登場などにより，ピア・ツー・ピアと称される技術に対し，関心が集まるようになってきた．

ピア・ツー・ピア(以下P2P)とは，対等な機能を持った端末同士が相互に接続されたネットワーク形態を指す．各端末がクライアントとサーバの両方の機能を持っているため，専用のサーバを必要と必要とせず，ネットワーク構成の動的な変化に対応できるといった特徴をもつ．

本研究ではこのP2Pを利用して，必要な情報をICカードの一種であるJava Cardにいれる事により，利用する端末の種類などにとらわれず，かつ安全な通信を行うことが可能なグループ構築の方法を提案する．

2　P2Pにおける問題点

P2Pおいて最大の問題点と言われているのがセキュリティである．P2Pではサーバ・クライアント方式のネットワーク形態とは異なり，ユーザ一人一人の管理を行うことが不可能であるため，自分が通信したいと思った相手と本当に通信を行っているのかどうかが分からない．よって無関係な第3者が通信相手のふりをする「なりすまし」が発生し，通信内容を盗聴，改竄される恐れがある．

また，P2Pでの通信では，その内容が無関係のピアを経由して通信相手までルーティングされる為，その途中段階で盗聴，改竄の危険性があるのである．

P2Pの問題点はセキュリティだけではない．一般的にP2Pの通信ではIPアドレスを使用して相手を指定し，通信を行う．よって自分と通信相手の両方のIPアドレスが同時に変更された場合，ネットワーク中で通信相手を探し出すのはもはや不可能に近い．また，通信したいピアがファイアーウォールの中に存在すると，ファイアーウォールの外からはみつけられないので発見することも不可能である．

3　提案

本稿ではピア・ツー・ピアネットワーク上においてJava Cardを利用する事により，使用する端末に依存せず，また，安全に協調作業を行うことを可能にするグループの構築法を提案する．

Java Cardとは，Javaの実行環境を実装したICカードであり，アプレットと呼ばれるアプリケーションをカード上で実行することが可能であり，また，データを内部に格納することができるといった特徴を持つ．

ユーザはJava Cardを携帯し，移動先でその場にある端末を利用して他のユーザとグループを構築し，協調作業を行う．

3.1　システム構成

本システムは次の3つの部分から構成される．

ベース部分 P2Pによる通信を行う．

サービス部分 グループメンバの発見と認証，通信の暗号化を行う．

アプリケーション部分 協調作業を行うアプリケーション．

このように，アプリケーションをベース部分とサービス部分から独立させて構成する事により，協調作業で使用するアプリケーションをグループ構築とは無関係に動作させることが可能である．

3.2　グループ構築までの手順

ユーザーは以下のように本システムを用いてグループを構築する．

1. ユーザがJava Cardをカードリーダライタにセットすると，ユーザが加入可能なグループの一覧が表示される．

*Reina Miyaji,Hiroaki Ohya,Yoko Sugawara,Ken-ichi Okada
†Faculty of Science and Technology,Keio University

2. 選択されたグループの「親」となっているピアを検索し，発見されれば親に接続要求を出す．もしグループのメンバが 1 人もネットワークにいなければ自らが親となり，別のメンバが来るのを待つ．
3. 親によって接続要求が許可されると，親側のシステムと相互認証を行う．
4. 認証が成功すればグループに加入し，グループ内での協調作業が可能となる．

3.3 グループメンバの発見

ユーザが使用する端末は常に同じであるとは限らない．よって各グループに固有の ID をふり，その ID によってグループメンバであるか否かを識別する．

グループメンバを P2P ネットワーク内で検索，発見することは検索範囲をある程度搾れば不可能ではないが，時間を要する上，その範囲内で発見できる可能性は低いと言える．

よって，本提案では，Rendezvous Point という特別なピアを利用する事により，グループメンバを検索する方法をとる．Rendezvous Point とは「待ち合わせ場所」のようなものであり，1 グループに対し 1 つの Rendezvous Point を設ける．この Rendezvous Point とは本システムで使用している P2P プラットフォームである" JXTA" により提供されている機能である．グループメンバは各々自分のグループの Rendezvous Point に接続することにより，他のメンバを容易に検索，発見しグループを構成する事が可能となる．

3.4 認証と通信の暗号化

本システムでは対称鍵を用いた認証方法を用いる．グループメンバはグループで共通の対称鍵をカード中に保有し，チャレンジ・レスポンス方式を用いて以下のような認証を行う．

$Response = h(Challange||SecretKey)$ [*] [†]

また，通信内容の暗号化は，認証に用いた乱数と対称鍵を利用してセッションキーをカード内で生成し，これを用いて端末上で共通鍵暗号による暗号化を行う．

4 実装

4.1 実装環境

提案したシステムを Java 言語を用いて実装した．P2P のプラットフォームとして JXTA[3] を採用した．P2P プラットフォームは 3.1 におけるベース部分に相当する．本システムは JXTA 上のサービスとして実装されているため，アプリケーションは JXTA 上で動作するアプリケーションが本システム上でそのまま利用できる．カードリーダには同じく Gemplus 社の GCR401 を利用し，カードリーダにアクセスする手段として OCF(OpenCard Frameworks) を用いた．セキュリティに関しては，暗号化するアルゴリズムとして RC4 を用い，一方向性ハッシュ関数として SHA-1 を用いた．

[*] $h()$ はハッシュ関数
[†] $||$ は連結を意味する

4.2 実装例

本システムを利用したアプリケーションの例として，オークションアプリケーションを実装した．メンバがグループに加入すると，現在グループ内で行われているオークションの一覧を閲覧することができ，それらに対して入札したり，また，自らがグループに対してオークションを開催できるようにした．

5 まとめ

本研究ではピア・ツー・ピアネットワークを用いて協調作業を行うために，グループ構築の際に必要な情報を Java Card にいれて携帯する事により，利用する端末の種類などにとらわれる事なく，かつ安全な通信を行うことが可能なグループ構築の方法を提案した．この提案により，ユーザはその場にある端末を利用してピア・ツー・ピアネットワーク上でアドホックにグループを構築し，安全に協調作業を行うことができるようになった．

今後の課題としては，サービス部分において，グループメンバ間でのアクセスコントロールを制御する事が可能になるようにする事と，グループのリソース管理についても考えていきたい．

参考文献

[1] Sun Microsystems
http://java.sun.com/products/javacard/index.html
2002/1/15

[2] Project JXTA
http://www.jxta.org/ 2002/1/15

[3] 山崎重一郎，岩尾忠重，塩内正利，和田祐二，岡田誠，荒木啓次郎
P2P 型エージェントプラットフォームにおける信用ドメインの構築について
マルチメディア，分散，協調とモバイル 2001
pp681-686.