モバイルアドホックネットワークにおける階層型認証機構の一検討

小原 奈緒子 †　　小口 正人 †
† お茶の水女子大学 理学部情報科学科

1. はじめに

近年，コンピュータ間の通信においてサーバを介さない P2P(Peer-to-Peer) 型通信が発展している．この P2P という通信形態を用いて，様々なアプリケーションが実装され，また JXTA のように汎用的な P2P プラットフォームの開発も行われている．一方で，携帯電話によるモバイルネットワークサービスや無線 LAN などのモバイル向けネットワークインフラの普及も急速に進んでおり，モバイル向け P2P サービスの実現に対する需要も高まっている．このようなサービスでは，不正なユーザや機器からの脅威を防ぐための認証処理が必要不可欠である．しかし固定基盤を持たない無線アドホックネットワークでは実用的な認証システムが実現されておらず，セキュリティ上の脆弱性が問題となる．そこで本研究では，モバイルアドホックネットワーク内におけるノード間の認証システムを検討する．階層的に構築されたグループ内での認証機構を利用し，実用的な認証システムを実現する実験を行う．

2. P2P 型通信システム

現在広く利用されているクライアント・サーバシステムでは，クライアントがサーバに接続することで特定のリソースが利用可能となる．一方，P2P 型通信システムでは，ネットワークを構成するコンピュータが対等に処理を行う．P2P 型通信システムの利点として，サービスを提供する責務をネットワーク上の全てのコンピュータが分担することで，単一障害によるサービス停止を回避できるという点が上げられる．この P2P 接続を利用し，インターネットなどの固定基盤ネットワークに接続できない環境において集まったノードがその場のみで構築するネットワークのことをアドホックネットワークという．アドホックネットワークはインフラネットワークが存在しない場面では有効であるが，高度なセキュリティ設定ができないなど機能が限られているという面もある．

3. 研究目的

固定基盤を持たないモバイルアドホックネットワークにおいて完全な認証を実現することは原理的に不可能であるが，全てのノードを等しく「未認証」とするより仮認証などを行い信頼度に差をつけた方が望ましい場合が多い．そこで本研究では，モバイルアドホックネットワークにおいて認証に段階を付けた階層型認証機構の適用モデルを提案し，それぞれのレベルに応じた安全なコンテンツのやりとりを可能にするシステムの構築を目的とする．

A Study of Hiearchical Authentication
in Mobile Ad-hoc Network
† Naoko Ohara, Masato Oguchi
Department of Information Sciences, Ochanomizu University

4. 階層型認証機構とその動作

本研究ではアドホックネットワーク内の階層型認証モデルを提案し，モバイル環境において有効な認証システムを構築する．このモデルは以下のように動作する．まず，あるピアがアドホックネットワーク内でだけ有効である ID などを入力し，仮の認証を行うことによって，このピアは一段階上のピアグループにジョインすることができる．ピアグループとはある共通なサービスの集合について合意しているピアの集合である．このピアグループはアドホックネットワークにおける認証レベルを決定する機能を持つ．次に，ピアグループがインフラネットワークに接続した時に本認証を行うことによりアドホックネットワークにおける仮認証の是非を判断し，本認証で認められたら認証レベルをさらに上げる．認証レベルが上がるごとにユーザが受けることのできるサービスが拡大する．提案モデルを図 1 に示す．

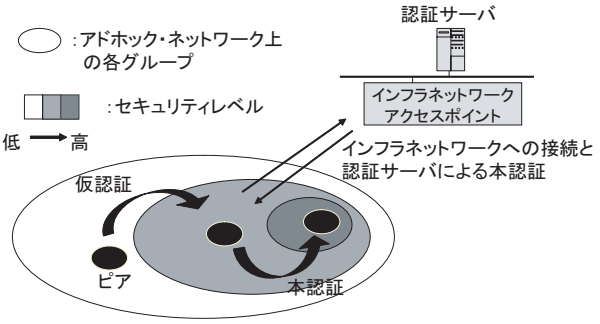

図 1: 提案モデル

5. 実験環境

本研究ではプラットフォームとして JXTA を使用した [1][2][3]．JXTA は言語独立でプラットフォームに非依存な P2P ソリューションを実現する汎用的フレームワークである．JXTA を利用することにより，P2P の細かい仕様を特別意識せずに P2P アプリケーションの構築が可能になる．JXTA において，ピアグループを作成するにはピアグループアドバタイズメントが必要であり，ピアグループの名前や ID，説明，仕様などが記述されている．各ピアグループは一意のピアグループ ID で識別され，ピアグループはそのピアグループ自身のメンバシップポリシを確立することができる．JXTA においてコミュニケーションのために使われる非同期かつ単方向のメッセージ転送機構はパイプと呼ばれる．JXTA ピアはメッセージを他のピアに送信するためにこれを使用する．

本実験ではノート PC 2 台にプラットフォームとして Linux2.4.18-14 と JXTAversion1.0 をインストールし，これらを IEEE802.11b 無線 LAN 接続して用いた．

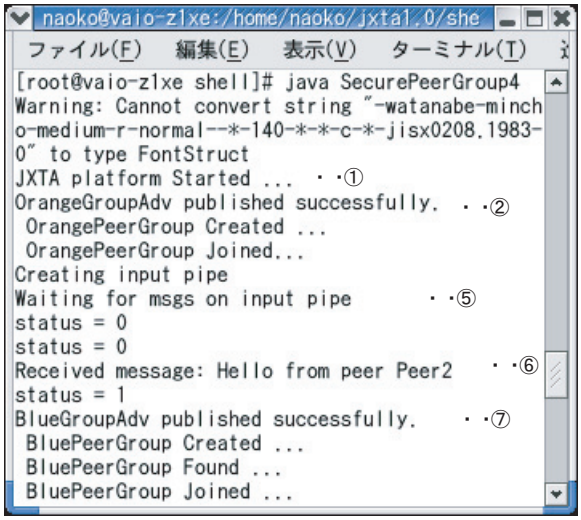

図 2: ピアグループ作成プログラムの実行結果

6. 実装プログラムの実験概要

本研究で JXTA を用いて実装したプログラムの流れは以下のようなっている．

- オープンなピアグループの作成
  デフォルトで全てのピアが所属しているネットピアグループのモジュール実装アドバタイズメントをコピーし，新しいピアグループのアドバタイズメントを作成，パブリッシュする．
- パイプの生成とメッセージの送信
  メッセージを受信する側では，新しいパイプアドバタイズメントを生成してそこから入力パイプを作り，その上でメッセージを入力待ちする．一方メッセージを送信する側では，新しいパイプアドバタイズメントを生成して出力パイプをつくり，そこから新しく作成したメッセージを送信する．
- メッセージの受信
  パイプに発生したイベントに関連するメッセージを取り出し，処理する．
- セキュアなピアグループの作成
  ログイン名とパスワードを用い認証機能を実装している新しいピアグループを生成，ジョインする．

このようにして，モバイルアドホックネットワークにおいて外部からの認証がなければセキュリティレベルの高いピアグループには参加できない階層型認証システムを構築した．

7. プログラムの実行

前章で述べたピアグループ作成プログラムの実行結果を図 2 に，JXTA ツールである JXTA シェルを用いて作成したピアグループを確認した結果を図 3 に示す．ピアグループ作成プログラムを実行すると，始めに JXTA プラットフォームを初期化し，デフォルトのネットピアグループを生成する [①]．次に，ネットピアグループを親

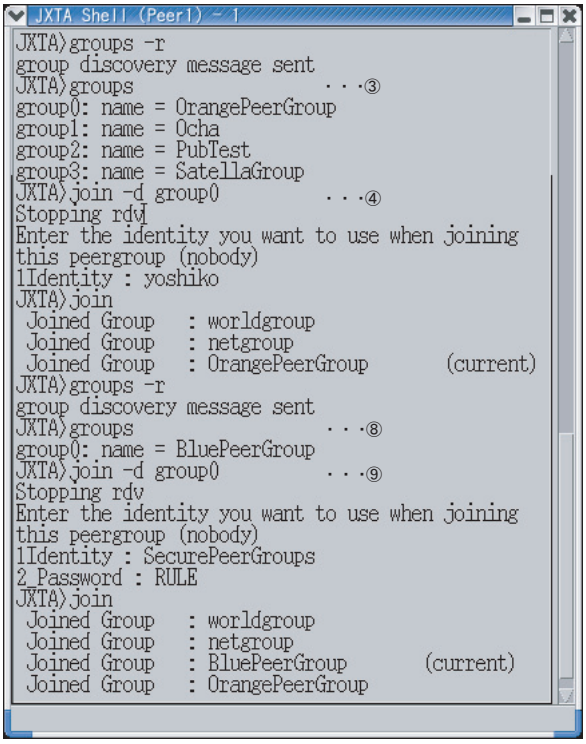

図 3: JXTA Shell における実行結果

ピアグループとして，誰にでも参加可能なオープンなピアグループを生成し，それに参加する [②]．この段階において，JXTA シェルを用いてオープンなピアグループ（OrangePeerGroup）が存在し [③]，これにジョインできることが確認できた [④]．次に，外部のノードからのメッセージを入力待ちし [⑤]，メッセージを受信することができたら [⑥]，オープンなピアグループを親ピアグループとしてセキュアなピアグループを生成し，それに参加する [⑦]．JXTA シェルでセキュアなピアグループ（BluePeerGroup）が存在し [⑧]，これにジョインできることが確認できた [⑨]．以上により，外部の認証を必要とする安全性の高い階層型認証システムが作成できた．

8. まとめと今後の課題

作成したプログラムを用いて，モバイルアドホックネットワーク内でより高度な認証を実現できることが確認できた．今後はこれを改良して，グループ数，セキュリティレベルを自由に設定できるプログラムを完成させ，それを利用してモバイルアドホックネットワーク環境で実用的な階層型認証を行うような全体的枠組みを表現するシステムを構築していく予定である．

参考文献

[1] http://translation.jxta.org/ja/mirror/www/docs/jxtaprogguide_final.pdf

[2] Brendon J.Wilson JXTA のすべて, 日経 BP 社

[3] http://tmasada2.hp.infoseek.co.jp/xml/JxtaProtocols.html