モバイルアドホックネットワークにおける認証機構の考察
A Study of Authentication in Mobile Ad-hoc Network

小原 奈緒子 †　　**小口 正人** †
Naoko Ohara　　Masato Oguchi

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[2][3] 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．無線 LAN などのモバイルネットワーク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に認証処理が必要不可欠である．しかしインターネットに接続されていない環境において一時的に構築されるアドホックネットワークでは，PKI(Public Key Infrastructure) を始めとする固定的な認証機構が利用できず，一般的な認証システムを用いることは困難である。ゆえに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っている．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，考察する．

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がモバイルアドホックネットワークである．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，インフラネットワーク接続時と同等の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．我々はこれまで，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てきた [4]. 本論文では，具体的な認証の手法を検討し，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．

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における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考察する．階層型認証モデルを検討するに当たり，その背景となる環境として，例えば無線 LAN のノード同士の通信であるアドホックネットワーク自身が移動している場合を考える．アドホックネットワークで接続された各ノードが電車や飛行機などに乗り合わせており，外界との接続が途切れることもあれば，アクセス・ポイントでインフラネットワーク（有線）に接続できる時もある．またアドホックネットワークを構築する前に，個々のノードが認証に関する何らかの情報をあらかじめ保持している可能性もあるものとする．そのような環境において，アドホックネットワークで接続されたノード同士がある会員サービスのメンバであるかどうか互いに認証する場面を考える．

4.1 認証手法 1

事前に有線に接続した状況において，ある会員サービスのメンバ同士がお互いの公開鍵を知ることができ，そのメンバがアドホックネットワーク内に移ってきた場面を考える．無線アドホックネットワーク内でメンバであるＡとＢが，元から知っていた互いの公開鍵を使って認証を行う．

1. Ａが自分の秘密鍵を使ってメッセージを暗号化し，それをＢに送る
2. ＡからＢがＡの公開鍵で復号化する

この逆の手順も行うことで，ＡとＢが互いに認証し合うことができる．この認証では，有線で接続された状況においてあらかじめお互いの公開鍵を知っているので，基本的に不正行為はできずセキュリティレベルは高い．しかし実際には，会員サービス内のメンバはＡとＢの二人だけではなく大勢いることが予想されるため，会員の公開鍵一覧を格納したデータベースが膨大な量になってしまう可能性が高い．また会員サービスに参加している人は入れ替わることが予想されるので，データベースを頻繁に更新しなければならない．従って一般には個々のノードが公開鍵一覧のデータベースを持ち歩くことはあまり現実的でないと考えられる．認証手法１は小規模な会員サービスでしか利用できないなど，適用できる場面が限られる．

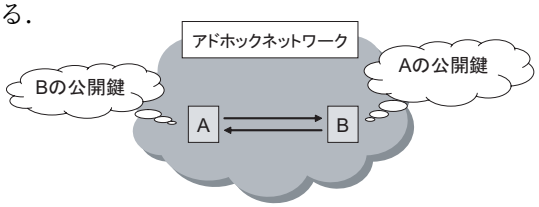

図 1: 認証手法１

4.2 認証手法２

個々のノードが公開鍵一覧のデータベースを持ち歩かなければならないという認証手法１の短所を解決するため，次のような認証手法２が考えられる．無線アドホックネットワーク内に会員サービスを提供している組織，あ

†お茶の水女子大学,Ochanomizu University

るいは委託を受けた組織が提供する認証ノードTが存在しており，個々のノードは互いの公開鍵を知らなかった場面を考える．ただし各ノードは認証ノードの公開鍵も知らないものとする．AとBは認証ノードTから公開鍵を受け取り，認証を行う．

1. BがTからAの公開鍵を受け取る
2. Aは自分の秘密鍵でメッセージを暗号化してBに送る
3. BがAから送られてきたメッセージをAの公開鍵で復号化する

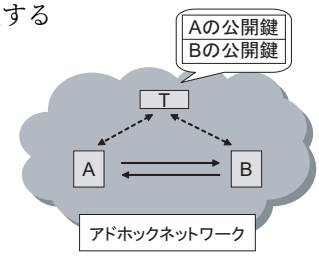

図 2: 認証手法 2

逆の手順も行うことで，AとBが互いに認証し合うことができる．この認証手法2では，あらかじめ個々のノードがお互いの公開鍵も認証ノードTの公開鍵も知らなかったため本物であるという確証が得られず，次のような場合が考えられる．以下，AとBが逆の場合も同様である．

case1: 認証ノードTが偽の場合

認証ノードTが偽の場合，TはAとBに本物の公開鍵を渡さないので，AとBは互いの認証を行うことができず，通信は成り立たなくなる．

case2: Bが偽の場合

Bが偽者である場合，Aは認証ノードTから正しいBの公開鍵をもらって復号化しようとするので，偽のBのメッセージはAによって認証されない．

case3: Bも認証ノードTも偽である場合

このケースでは，偽のBと偽の認証ノードTが共謀して不正を行おうとする．偽のBは自分の秘密鍵を使ってメッセージを暗号化し，AはTから送られてきたBの偽の公開鍵を使って復号化，認証してしまう．

この認証手法2には次のような問題が存在する．アドホックネットワークに参加した時に認証ノードTがたまたま存在する可能性は高くない．また，認証手法2ではTとBが共謀すれば，不正を行うことができてしまう．従ってそれはセキュリティレベルの低い認証とみなし，価値の低いコンテンツ（数百円程度の音楽データなど）の通信のみを行うことが適切といえる．このセキュリティレベルの低さを解消する改善策としては，アドホックネットワークがアクセスポイントなどでインフラネットワークに接続できた時に認証ノードTが正しいかどうか判断するなどの方法が考えられる．

4.3 認証手法3

認証手法2ではあらかじめ個々のノードが認証ノードTの公開鍵を知らなかったため，セキュリティレベルの低い認証しか行えなかった．認証手法3では，あらかじめ有線に接続できる状況において会員サービスのメンバが認証ノードTの公開鍵を知ることができ，そのメンバがアドホックネットワーク内に移動してきた場面を考える．無線アドホックネットワーク内で会員であるAとBが，あらかじめ知っていた認証ノードTの公開鍵を用いてTを認証する所から始める．

1. Bは認証ノードTよりTの秘密鍵で暗号化されたメッセージを受け取り，Tの公開鍵で復号化して，Tの認証を行う．
2. BがTからAの公開鍵を受け取る
3. Aは自分の秘密鍵でメッセージを暗号化してBに送る
4. BがAから送られてきたメッセージをAの公開鍵で復号化する

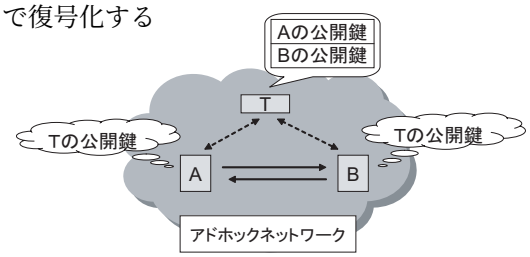

図 3: 認証手法 3

逆の手順も行うことで，AとBが互いに認証し合うことができる．この認証手法3では，認証手法1と違い，会員サービスのメンバが知っておかなけらばならないのは認証ノードTの公開鍵だけなので，膨大なデータベースを持ち歩く必要はない．また，メンバがあらかじめ認証ノードTの公開鍵を知っているため基本的に不正を行うことはできず，セキュリティレベルが高い．

本研究では上記の認証手法2と認証手法3を用いて次のような階層型認証モデルを提案する．同じレベルのサービスを受けるピア（ノード）の集まりをピアグループと呼ぶが，会員サービスのメンバがこのピアグループに属しているという場面を考える．複数のピア同士が，誰でも所属可能であるオープンなピアグループを形成している時はコンテンツのやり取りは許可されない．しかし，ピアグループ内でたまたま存在する認証ノードを見つけて認証手法2を行った際には，低いレベルで認証が行われ，価値の低いコンテンツのやり取りだけが許可される．さらに，セキュリティレベルの高い認証手法3を行うことができた場合には，価値の高いコンテンツのやり取りが可能になる．このように，属しているピアグループの認証レベルの階層が上がるごとに，ユーザが受けることのできるサービスが拡大する．

5. まとめと今後の課題

本研究ではアドホックネットワーク内で有効であると考えられる階層型認証モデルを提案した．今後の課題としては，認証レベルに応じたサービスを受けられるような階層型認証機構を JXTA プラットフォームなどに実装したいと考えている．

参考文献

[1] ブルース・シュナイアー，暗号技術大全，ソフトバンク

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

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

[4] 小原奈緒子，小口正人：”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 ”，情報処理学会 第 6 回 全国大会，2T-8,2005 年 3 月