MANETにおける公開鍵暗号方式を用いた階層型認証システムの提案と実装

小原　奈緒子†　　小口　正人†

† お茶の水女子大学　〒 112–8610 東京都文京区大塚 2–1–1
E-mail: †naoko@ogl.is.ocha.ac.jp,†oguchi@compter.org

あらまし　本研究では，モバイルアドホックネットワーク（MANET）において公開鍵暗号方式を用いた階層的な認証システムを提案・実装する．本研究は MANET 内で会員サービスのメンバが安全にコンテンツのやり取りを行うことができることを目標としており，そのためには認証システムが必要となる．ただし，固定基盤を持たないモバイルアドホックネットワーク (MANET) 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．しかし，全てのノードを等しく「未認証」とするより，完全ではないがある程度の信頼性を持つ認証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, セキュリティレベルの異なる認証手法を組み合わせて次のような階層型認証機構を構築する．MANET 内の個々のノードは同じ会員サービスに属するメンバをセキュリティレベルによって格付けし，そのリストを保有する．認証要求が発生した際に，公開鍵暗号方式を用いて相手を認証し，その認証のセキュリティレベルに応じて相手をランク付けしてリストに追加する．このシステムを用いることにより認証レベルが上がるごとに受けることのできるサービスが拡大し，セキュリティレベルに応じたサービスを受けることができる枠組みが構築可能になる．

キーワード　セキュリティ，アドホックネットワーク，モバイルコンピューティング，認証，公開鍵暗号

Proposal and Implementation of Hierarchical Authentication System with Public Key Cryptosystem in MANET

Naoko OHARA† and Masato OGUCHI†

† Ochanomizu University　Otsuka 2–1–1, Bunkyo-ku, Tokyo, 112–8610 Japan
E-mail: †naoko@ogl.is.ocha.ac.jp,†oguchi@compter.org

Abstract　In this paper, we propose and implement a hierarchical authentication system with public key cryptosystem in MANET. Our goal is that members of membership services in MANET can give and take their contents safely. To accomplish it, although authentication system is necessary, it's impossible to achieve complete authetication equivalent to authentication in an infrastructure network. However, it's more desirable to do inexhaustive authentication and hierarchize credibility rather than to do nothing. Therefore, we combine defferent levels of authentication methods and develop hierarchical authentication system as follows. Each node in MANET grades security level on members in the same membership service and possess the list. When other members call for authentication, the member authenticate them with public key system and add them to the list according to the authentication level. With this system, the service that members enjoy can be increased as the level is raised. Thus members can enjoy services depending on thier security level.

Key words　security, ad-hoc network, mobile computing, authentiction, public key cryptosystem

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階層型認証システムを提案し，公開鍵暗号方式を用いて実装する．

2. 研究背景

2.1 モバイルアドホックネットワーク

現在インターネットでは多くの場合，クライアント・サーバ型システムが用いられている．このクライアント・サーバ型システムではクライアントがサーバに接続して特定のリソースへのアクセス権を得る．しかしサービスを提供するための処理の大部分はサーバで行われるため，クライアントの数が増えるにつれサーバの負荷が増大してしまい，過負荷になるとシステム全体がダウンしてしまう可能性がある．そこで P2P 型通信システムが有効になる．このシステムでは中央サーバを設けず，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．サービスを提供する責務をネットワーク上の全てのノードが分担するので，単一障害によるサービス停止を回避できる．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を MANET(モバイルアドホックネットワーク) と呼ぶ. これ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．

2.2 公開鍵暗号方式

公開鍵暗号方式とは公開鍵と秘密鍵という対になる二つの鍵を使って暗号化・復号を行う方式である [1]. 片方の鍵を使って暗号したものはもう片方の対となる鍵を使わなければ復号できないという特徴を持つ. この特徴を生かすとあらかじめ暗号通信のために鍵を共有しておく必要がなくなり，また 1 つの鍵で複数の相手との暗号通信が可能になる．例として A が B に文書を送る場合を考える．B は自分の公開鍵と秘密鍵を作成し，公開鍵だけを一般に公開する．A は B の公開鍵を入手して文書を暗号化して B に送る．受け取った B は自分の秘密鍵で復号する．送られた文書は B の秘密鍵でしか復号できないため，B だけがその文書を読めることになる．公開鍵暗号方式を暗号通信とは逆の方法で利用したのが電子署名である．A が B に対しある文書を送ろうとしている時，文書を自分の秘密鍵で暗号化した署名を文書と共に送る．この 2 つを受け取った B は、まず暗号化された署名を A の公開鍵で復号し，それと文書を比較する。これが一致すれば，その文書は改ざんされていないということが言える．公開鍵を用いて復号できるということは対応した A の秘密鍵で暗号化されたということなので，暗号化したのは A に間違いないという図式が成り立つからである．

2.3 JXTA

JXTA はサン・マイクロシステム社が開発した P2P 型のシステムを構築するための代表的なプロトコル及びツール群である．JXTA 論理レイヤの下位層である JXTA コアや JXTA サービスが P2P の基本的枠組みを提供しているため，その詳細な知識を持っていなくても上位層である JXTA アプリケーションで P2P アプリケーションを開発することができる．JXTA においてある共通なサービスについて合意しているピアの集合をピアグループと言う．全てのピアは JXTA で常に存在する NetPeerGroup に属し，その他のピアグループへジョインすることも選択できる．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，これにはピアグループの名前や ID，仕様などが記述されている．JXTA ピアは，メッセージを他のピアに送信するために JXTA パイプサービスを使用する．パイプはサービスのコミュニケーションのために使用される非同期かつ単方向のメッセージ転送機構である．受信点である入力パイプと送信点である出力パイプをエンドポイントとして，メッセージを送受信する際にピアのエンドポイントと動的にバインドする．

3. 研究目的

本研究では，MANET 内で会員サービスのメンバが互いに認証を行い安全にコンテンツのやり取りを行うことができるシステムの構築を最終的な目標としている．ピアは属する会員サービスの種類によって異なる ID を持っていて，この ID を申告しあうことによって図 1 のように MANET 内でピアグループを形成し，通信をはじめる．このピアグループ内でメンバが安心してコンテンツのやり取りを行うためには認証することが必要となる．ただし，固定基盤を持たない MANET 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．しかし，全てのノードを等しく「未認証」とするより，完全ではないがある程度の信頼性を持つ認証（以下仮認証）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，MANET において認証に段階を付けた階層型認証機構のモデルを提案し，具体的な認証手法を検討してきた [4] [5] [6]. 本論文では，これまで提案した手法を基に、MANET における認証モデルとその実現方法を議論し、公開鍵暗号方式を用いて実用的な認証システムを実装する．そしてセキュリティレベルに応じた安全なコンテンツのやり取りを行うシステムを実現する．

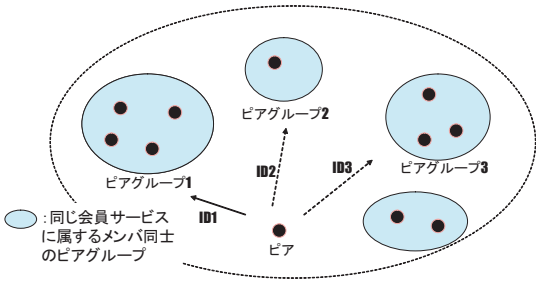

図 1　会員サービスへの参加

4. モバイルアドホックネットワークにおける認証手法

階層型認証機構を議論するにあたり，まず初めに完全な認証や仮認証といったレベルの異なる認証手法をそれぞれ提案する．

MANET においてある会員サービスに属しているメンバが認証し合い，コンテンツをやり取りする場面を考える．会員サービスのプロバイダは公開鍵などの会員情報を保持しており，会員は有線に接続した状態においてそれにアクセスすることが可能である．また，モバイルユーザが列車に乗り合わせた場合など，MANET 自体が移動している場面では、断続的にアクセス・ポイントでインフラネットワークに接続できる可能性もある。一方，MANET 内において個々のノードが他のノードの公開鍵などの認証に関する何らかの情報をあらかじめ保持している場合もあるものとする．以下の議論においては，正しい公開鍵で認証されたノードは MANET 内で会員サービスに属しているメンバに対して不正を行わず，正しい情報のやり取りを行うものとする．また，データの改ざんを防ぐため，公開鍵暗号方式を用いて通信自体も暗号化する．

4.1 認証手法 1

公開鍵を知っていたメンバが MANET 内に居合わせる場面を考える．Aが元から知っていたBの公開鍵を使ってBの認証を MANET 内で行う (図 2).

（1） B が自分の秘密鍵を使ってメッセージを暗号化し，それを A に送る

（2） B から送られてきたメッセージを A が B の公開鍵で復号する

この時Bの公開鍵で復号できれば B だけが持つ秘密鍵で暗号化されたということが言えるので認証が成立したことになる．この逆の手順も行うと，AとBが互いに認証し合うことができる．

この認証では，MANET を形成する前から知っていた公開鍵を使って認証を行ったので，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メンバ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，個々のノードが会員全員の公開鍵一覧のデータベースを持ち歩くことは一般的に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．

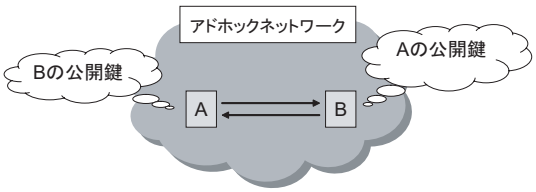

図 2 認証手法 1

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，公開鍵を知らないメンバが居合わせる場合を考える．AはBの公開鍵を知らなかったので，MANET 内でBの公開鍵を知る第三者であるノードを探す．以下の議論においてこのノードをTと呼び，Tは単数または複数の場合があり，サービスプロバイダ公認のノードであるケースも含まれる．

この時探されるノードをTと呼び，はサービスプロバイダ公認のノードであるケースも含まれ，AはTの公開鍵を知らなかったものとする．AはTからBの公開鍵を受け取り，Bの認証を行う (図 3).

（1） AがTからBの公開鍵を受け取る

（2） Bは自分の秘密鍵でメッセージを暗号化してAに送る

（3） AがBから送られてきたメッセージをBの公開鍵で復号する

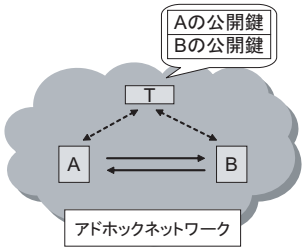

図 3 認証手法 2

認証手法 2 では，あらかじめ個々のノードが互いの公開鍵もTの公開鍵も知らなかったためそれが本物であるという確証が得られず，次のような場面が考えられる．以下，AとBが逆の場合も同様である．

case1: Tが偽の場合

T が偽の場合，T は A に本物の公開鍵を渡さないため B の認証を行うことができない.

case2: Bが偽の場合

Bが偽である場合，AはTからBの正しい公開鍵をもらって復号しようとした際に B が偽であることが分かる

case3: BもTも偽である場合

このケースでは，偽のBと偽のTが共謀して不正を行うことが可能である．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すると，認証が成立してしまう．

この認証手法 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仮認証とみなし，価値の低いコンテンツ（例えば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決する方法としては，MANET 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ノードTや B の公開鍵が正しいかどうか判断するなどの対策が考えられる．

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，MANET 内にBの公開鍵を知るTが存在し，Aがあらかじめ T の公開鍵を知っていた場面を考える．A が，あらかじめ知っていたTの公開鍵を用いてTを認証する所から始める (図 4).

（1）　A は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の公開鍵で復号してTの認証を行う

（2）　A はTから B の公開鍵を受け取る

（3）　B は自分の秘密鍵でメッセージを暗号化して A に送る

（4）　AがBから送られてきたメッセージを B の公開鍵で復号する

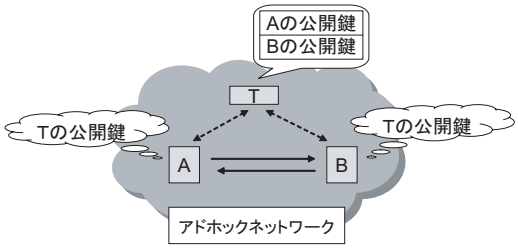

図 4　認証手法 3

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．さらに，T が正しいかどうかを確認できてから B の認証を行うため，基本的にどのノードも不正を行うことはできず，セキュリティレベルが高い．

5.　認証手法の階層型認証機構への適用

5.1　階層型認証機構の基本的枠組み

本研究では前節で述べた認証手法を利用することによって，次のような階層型認証機構を提案する．

個々のノードは MANET を形成する前から同じ会員サービスに属するメンバの公開鍵を知っている場合があり，それは公開鍵リストに格納される．会員サービスのメンバは有線に接続した状態で，適当なメンバとその公開鍵を公開鍵リストに入れることができる．また，個々のノードは同じ会員サービスに属するメンバをセキュリティレベルで格付けし，ピアグループ内でそのメンバと公開鍵に関する情報を保有する．これをセキュリティテーブルと呼ぶ．これはメンバそれぞれによって異なる相対的なものであり，ピアグループにジョインする度に生成される．このセキュリティテーブルは高，中，低の三段階のセキュリティレベルを持ち，それは格納されているノードが会員サービスに属している可能性はどの程度であるかを示す．あるノードが他のメンバを認証する際に，信用できる公開鍵によって認証が成立した場合には相手とその公開鍵を高レベルに，そうでない場合は中レベルに相手を追加する．この時，信用できる公開鍵とは公開鍵リスト，もしくは高レベル層にいるメンバの公開鍵のことを指す．信用できるとは言えない公開鍵とはその他全ての公開鍵を指し，公開鍵リストにはなく，高レベル層にも存在しないメンバの公開鍵のことである．また，公開鍵が分からないため，自己申告した ID を用いてオープンな認証のみを行った場合にはそのメンバの ID を低レベルに追加する．

例えばピアグループ内にジョインしたばかりのAがBを認証する場合を考える．図 5 がAの持つリストであると考えると，Bが ID を申告してピアグループにジョインしてきた際にはまず低レベル層にBの ID を追加する．しかし，たまたま居合わせたTを用いて認証手法 2 を行うことができたら中レベル層にBとその公開鍵を追加し，Bのセキュリティレベルを上げる．さらに有線においてTの公開鍵が正しいと確認できたら認証手法 3 を行い高レベル層までBとその公開鍵をレベルアップさせる．ただし，Bがまだ低レベル層にいた段階でセキュリティレベルの高い認証手法 1 や認証手法 3 を行うことができた場合には飛び越えて一気に最高レベルまで上げる．

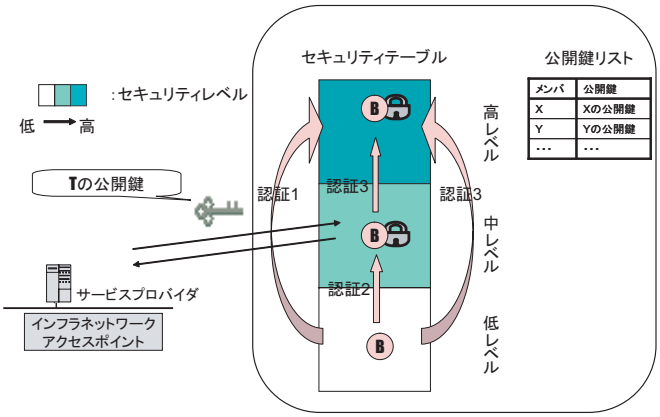

図 5　階層型認証機構の提案モデル

会員サービス内の個々のメンバがそれぞれ前節で述べたセキュリティテーブルを保有し，それを参照し合うことによって本研究の階層型認証システムは成り立つ．信用できる公開鍵によって認証した相手を高レベルに追加した際には，その相手が持つセキュリティテーブルを参照して自分のものを更新する．この際には次のルールに従う．

- 相手のテーブルのみに存在するノードとその公開鍵を追加
- 自分と相手両方のテーブルに存在するノードには，より高いレベルを適用

このように信用できる相手のテーブルを参照することにより更新されたデータも，自分が認証して得たデータと同様に扱う．従って，相手のセキュリティテーブルを参照することによって高レベル層に追加されたメンバ情報も認証を行う際に信用できるものとして利用される．中レベル層に追加された情報は高レベル層のものよりセキュリティレベルが低く，低レベル層に追加された情報はさらに低い．このような過程を経ると，会員サービスのメンバは直接コンタクトを取った数より多くのメンバのセキュリティレベルを知ることになり，信頼の輪が広がっていく．

5.2　動作アルゴリズム

前節で述べた内容に基づき，本研究で提案した階層型認証シ

ステムは次のようなアルゴリズムに沿って実行される．

ピアグループ内にいる他のメンバを認証する際のアルゴリズムを以下に示す．A が自分のセキュリティテーブルや公開鍵リストを利用して B を認証するとする．B から認証要求があった際には，A はまず B が自分のセキュリティテーブルの高レベル層に存在するかどうかを確かめる．この時 B を高レベル層に発見した場合にはその B の公開鍵を用いて認証を依頼した B が本物であるかどうかを確認するだけでよい．しかし B を高レベル層に発見できなかった場合には，B のセキュリティレベルを上げることができる可能性があるので次のようなプロセスを経る．

まず B が自分の公開鍵リストに存在するかどうかを確認する．もし自分の公開鍵リストに B が存在したら，認証手法 1 を行い B を高レベル層に認定する．もし自分の公開鍵リストにはなかったら B の信用できる公開鍵を知っているノードである T を探す．T が見つかったら，T がどの程度信用できるかを判断するために，まず自分の公開鍵リストやセキュリティテーブルを見る．この時 T を自分の公開鍵リストまたはテーブルの高レベル層に発見したら T は信用できると判断する．信用できると判断される T が保持する信用できる公開鍵は信用することができるため，A は B に対してセキュリティレベルの高い認証を行うことができる．この認証は認証手法 3 に相当するので，B と T を高レベル層に認定することができる．

しかしセキュリティテーブルの中レベル層または低レベル層に T を発見したり，もしくはテーブル内に T が存在しなかった場合もある．この時 T は信用できるとは言えないので，T の教えてくれた B の公開鍵により，B に仮認証を行う．これは認証手法 2 に相当するので，B を中レベルに認定する．この際にもし有線に接続して B の公開鍵を確認することができたら，より高い認証を行い B を高レベルに上げることができる．

MANET 内で T を探したが，B の公開鍵を知る人が誰もいなかった場合も考えられる．この時 A は B のセキュリティレベルを上げることはできないが，B が ID を申告することにより B を低レベルに追加することはできる．以上に述べた動作をまとめると，次のアルゴリズムとなる．

[認証とセキュリティレベル更新に関するアルゴリズム]

```
if(高レベル層に B が存在) {
  高レベル層にある公開鍵を用いて B を確認
}else{
  if(A の公開鍵リストに B が存在) {
   認証手法 1 で高レベルへ B を認定
  }else if(公開鍵リストに B がない) {
    信用できる B の公開鍵を知っている T を探す
   if(T が見つかった) {
      if(T が A の公開鍵リストまたは高レベル層に存在) {
        認証手法 3 で B と T を高レベルに認定
      }else{
        認証手法 2 で B を中レベル層に認定
        if(有線で B の公開鍵の情報を取得) {
          B の公開鍵を確認して認証手法 3 を行い B を高レベル層に更新
        }
      }
    }else if(T が見つからなかった) {
      if(A の中レベルに B がいる) {
        中レベル層にある公開鍵を用いて B を確認
      }else{
        A のテーブルの低レベルに B を認定
      }
    }
  }
}
```

次に他のメンバのセキュリティテーブルを参照する際のアルゴリズムを以下に示す．A が B を認証し，自分のセキュリティテーブルに加えた後，そのレベルによって B のテーブルを参照するかどうか判断するところから始まる．

もし，B が自分のテーブルの高レベルに認定されたら B はセキュリティレベルの高い認証に合格し，信用できるということが言える．よって B のテーブルを参照して自分のテーブルを更新し，同じピアグループにジョインしているより多くのメンバのセキュリティ情報を得る．その際の手順としては，もし自分のテーブルには存在せず B のテーブルにだけ記載されているメンバがいたら，そのメンバと公開鍵を B のテーブルと同じレベルで自分のテーブルに追加する．もし，自分と B 両方のセキュリティテーブルに存在するメンバがあったら，両方のテーブルを比べて次のようにレベルの高い方を適用する．同じメンバが自分のテーブルでは B のテーブルよりも高い層にいたら，そのままにする．一方逆の場合には自分のテーブルを更新し，B のテーブルと同じレベルまでそのメンバを上げる．こうすることで，そのメンバに対してよりセキュリティレベルの高い認証をできた方が採択される．

しかしもし B が高レベル層に認定されなかった場合には，B は偽の会員メンバである可能性があり，その情報はある程度の信頼性しか持たない．よって B のテーブルを参照しない．以上のセキュリティテーブル参照と更新をまとめると，次のアルゴリズムとなる．

[セキュリティテーブル参照と更新のアルゴリズム]

```
if(B を高レベルに認定) {
  B のテーブルを参照{
        if(B のテーブルにだけ存在するノードがある) {
          そのメンバと公開鍵を B のテーブルと等しいレベルで A のテーブルに追加
        }else if(A と B 両方のテーブルに存在するノードがある) {
          より高いレベルを適用してそのノードを A のテー
```

ブル内で更新
        }
    }
}else if (Bを中レベルもしくは低レベルに認定){
  Bのテーブルを参照しない
}

個々のノードは公開鍵で暗号化したコンテンツをピアグループ内でやり取りする．その際には，自分のセキュリティレベルに応じたサービスを受けることができる．例えば音楽配信サービスを例にあげると，Bが低レベル層にいる時には曲のイントロしか受け取ることはできない．しかし，中レベルに上がるとより多くの音楽情報を受け取ることができ，最高レベルでは全てのコンテンツを利用できるようになる．このように認証レベルが上がるごとにBが受けることのできるサービスは拡大され，セキュリティレベルに応じたサービスを受けることができる．

5.3 階層型認証機構の適用例

この階層型テーブルを利用した認証システムがどのように動作するか具体例を図 6 に示す．

①まず初めにBがAに認証要求を出したとする．B がセキュリティテーブルにも公開鍵リストにも存在しなかったのでAはBの信用できる公開鍵を知っているノードを探す．D がBの公開鍵を知っていると報告したので，D にそれを教えてもらうことによって認証手法 2 を B に実行する．B が確認できたら中レベルにアップさせる．

②次に C が A に認証要求を出したとする．A は自分が持っている公開鍵のリストの中に C の公開鍵を見つけたのでそれを利用して認証手法 1 を C に適用する．C が正しいと判明したら高レベルに追加する．

③この時，高レベルにいる C は信頼できると言えるので C のセキュリティテーブルを参照して A のテーブルを更新する．A のテーブルには存在しなかった E と D が新たに追加される．C と A のテーブルを比較すると，B に対して C は A よりも高度な認証を行うことができたことが言えるため，A のテーブルにある B の公開鍵が C のテーブルにある B の公開鍵と等しいことを確認して，A は B のレベルを上げる．このセキュリティテーブルの情報を利用することにより，それぞれのメンバは自分のセキュリティレベルに応じたサービスを受けることができる．この時点では低レベルにいる D は少しのサービスしか受けられない．中レベルにいる E はコンテンツの一部を受け取ることができる．さらに高レベルの C と B は全てのコンテンツを A から利用できる．

④次に D が認証要求を出したとする．D のセキュリティレベルはまだ低レベルだったので A は D をレベルアップさせようと試みる．D が A の公開鍵リストに存在しなかったので，D の信用できる公開鍵を知っているノードをピアグループ内で探す．ここで E が D の公開鍵を知っていると報告してきたとする．A は E を自分のテーブルの中レベル層に発見したので，E は完全には信用できないと判断する．その E に教えてもらった D の公開鍵を用いて仮認証を行う．これは認証 2 に相当するので，認証が成功したら D は中レベルにレベルアップできる．

⑤仮認証を行った後に有線に接続できる状態になったとする．A は有線に接続し，サービスプロバイダの会員メンバの情報から E のデータを引き出し，E の公開鍵が正しいということを確認する．

⑥確認できたら E の公開鍵は信用できるということが言えるので，それを用いて A は D に対して認証 3 を行うことができる．認証が成功したら，A は D と E を高レベル層にレベルアップさせる．この時，高レベルにレベルアップした C,B,D,E は A から全てのコンテンツをもらうことができる．このような過程を経て信頼の輪が広がっていくモデルを提案する．

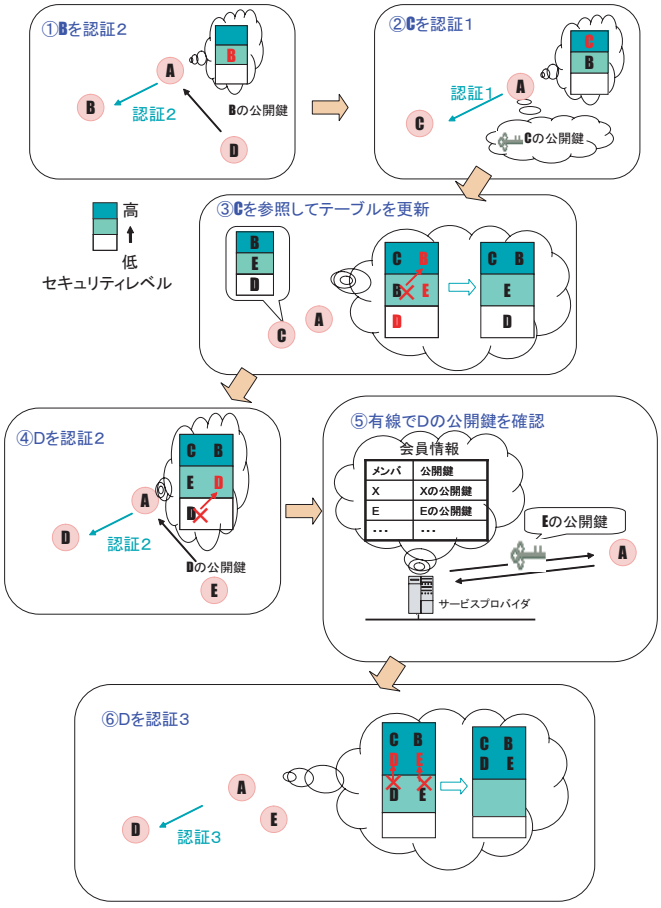

図 6　提案モデルの動作の具体例

6. 階層型認証システムの実装

本研究では階層型認証機構を実現するために，その個々の認証手法と階層的枠組みのプログラムを実装した．この二つのプログラムを利用し，MANET 内で有効な階層型認証システムを構築することを最終目標とする．

6.1 実験環境

図 7 のように 3 台の PC にプラットフォームとして JXTAversion2.3.3 をインストールし、これらを IEEE802.11b 無線 LAN で接続した．

6.2 認証手法のプログラムの概要

本研究では提案した認証手法 1 のプログラムについて説明

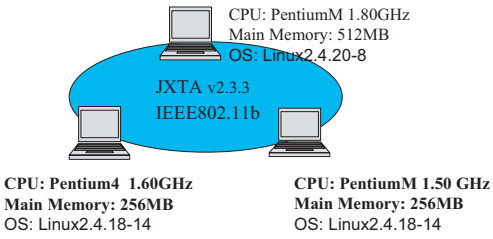

図 7　実 験 環 境

する．

1. 署名を生成

（1）　公開鍵と秘密鍵のインスタンスを作成

（2）　generateKeyPair() 関数を用いて公開鍵と秘密鍵のペアを作成

（3）　メッセージを秘密鍵で暗号化して署名を生成

2. メッセージと署名の送受信

まず受信側プログラムは入力パイプを生成しその上でメッセージと署名を入力待ちする．一方送信側では出力パイプを生成し，そこから JXTA パイプサービスを利用してメッセージと署名を送信する．出力パイプから送信されたメッセージと署名は入力パイプで受信される．

3. メッセージの検証

（1）　検証するための関数 Verify() を公開鍵を指定して初期化

（2）　署名を復号し元のメッセージと比較，検証

（3）　検証の結果を出力

6.3　認証手法のプログラムの実行結果

前節で述べた認証手法 1 のプログラムの受信側の実行結果を図 8 に，送信側の実行結果を図 9 に示す．初めに受信側でパイプサービスのアドバタイズメントを読み込んで入力パイプを生成しメッセージが届くのを待つ [①]．次に，送信側のプログラムが公開鍵と秘密鍵のペアを生成し，署名を作成する [②]．そしてパイプアドバタイズメントを読み込んで出力パイプを作成し，メッセージを送信する [③]．受信側がメッセージを受信し終わったら [④], 送信側が次に署名を送信する [⑤]. 署名を受信し終わったら [⑥] メッセージを署名と検証しその正否を出力する [⑦]. 以上により，P2P の環境において公開鍵暗号方式を用いて認証手法 1 を構築した．

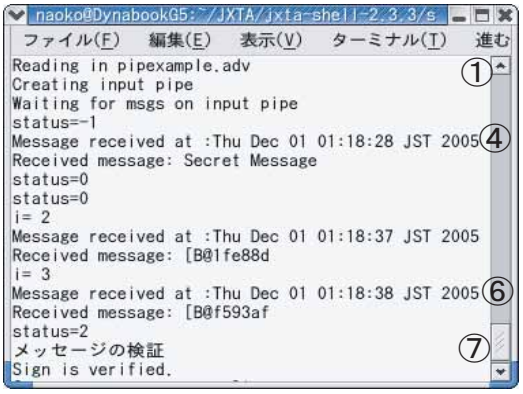

図 8　受信側プログラム実行結果

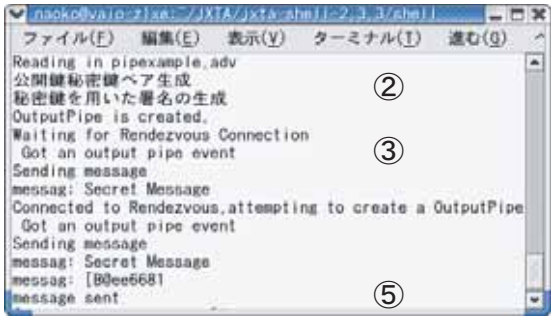

図 9　送信側プログラム実行結果

6.4　階層型認証のプログラムの概要

この JXTA プログラムはセキュリティレベルの異なるピアグループを用いて図 10 の階層的な認証を行う．この時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．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，レベルの低い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．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する．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．

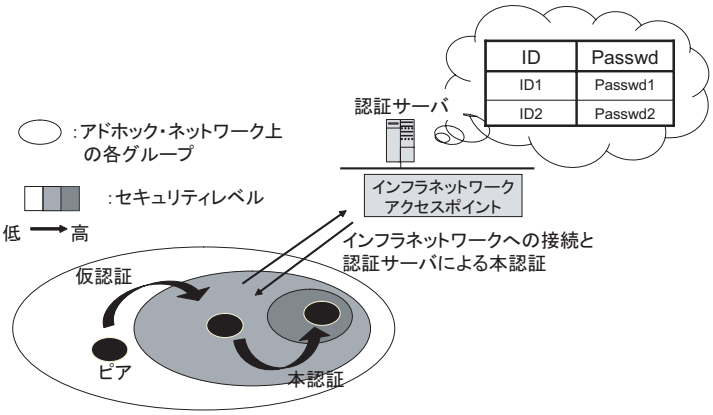

図 10　階層型認証を行う JXTA プログラムの動作

階層型認証の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．

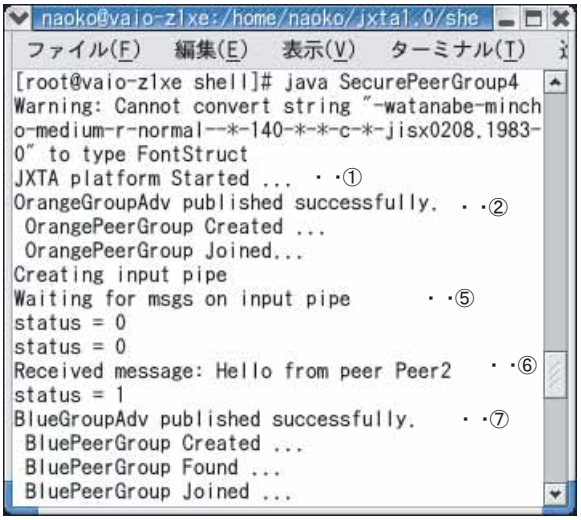

図 11　ピアグループ作成プログラムの実行結果

- セキュアなピアグループの作成

認証サーバから受信した情報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インフラネットワークに接続した場合にセキュリティレベルの高いピアグループに参加できる階層型認証システムを構築した．

6.5　階層型認証のプログラムの実行

前節で述べたピアグループ作成プログラムの実行結果を図 11 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 12 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，インフラネットワークへ接続した場合に高いレベルの認証が行える階層型認証システムが作成できた．

7.　関 連 研 究

文献 [7] [8] では認証局 (CA) の機能をネットワークに参加しているノードに対して分散させてローカルな CA を構築するメカニズムが提案されている．自分の公開鍵や認証情報に対して証明書を発行してほしいノードは周りの N 台以上のノードからそれぞれの”secret share”を集めて，それを合成した場合に限って正当な証明書の発行ができる．これらの論文では MANET 内で証明書が発行されるか否かで判断が二分される．しかし本研究では認証か未認証かに二分せず，インフラネットワークに接

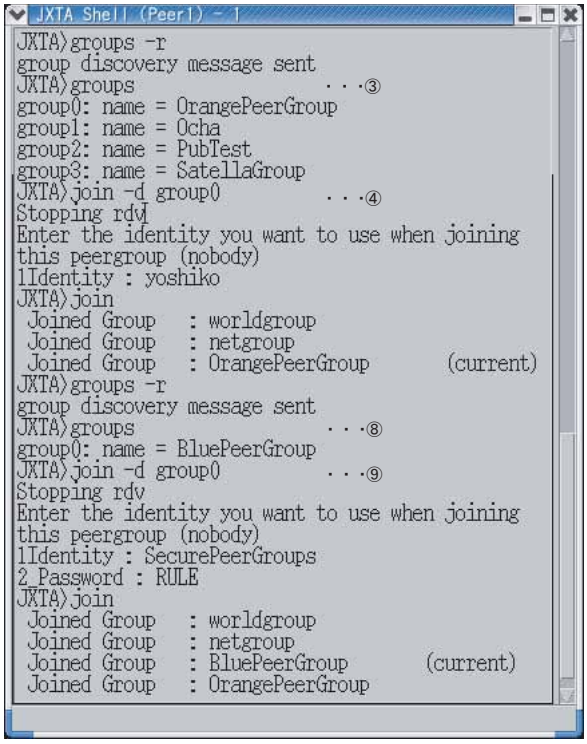

図 12　JXTA Shell における実行結果

続していない状態で MANET 内にある情報を用いてある程度のレベルを持つ仮認証を行う．そして認証に段階を付け，それぞれのレベルに応じたサービスを提供する枠組みを設けた．

8.　まとめと今後の課題

本研究では，MANET 内で有効であると考えられる階層型認証システムを提案し，その枠組みとレベルの異なる個々の認証手法を実装した．今後は提案モデルを改良すると同時に，実装したプログラムを利用して高度で実用的な階層型認証機構を JXTA プラットフォーム上で実装していきたい．

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://www.jxta.org/docs/JxtaProgGuide_v2.3.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

[5] 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認証機構の考察 ”，第四回情報科学技術フォーラム（FIT2005）,L-051,pp.125-126,2005 年 9 月

[6] Masato Oguchi,Yoshiko Nakatsuka, Chiho Tomizawa: “ A Proposal of User Authentication and Content Distribution Mechanism Using P2P Connection over a Mobile Ad Hoc Network”,IASTED CSN2004

[7] Alfarez Abdul-Rahman “ The PGP Trust Model ”, EDI-Forum: The Journal of Electronic Commerce,Volume:3,pp.27-31,Vol:10, April 1997

[8] H.Zhou and Z.Haas: “ Securing ad hoc networks ”, IEEE Networks, 13(6):24-30 (1999)