P2P フレームワークにおける公開鍵暗号方式を用いた認証機構の実装

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[1][2] 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．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，P2P フレームワークにおけるノード間の階層型認証システムを提案し，公開鍵暗号を用いて実装する．

2. 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 (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が，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モデルを提案し，具体的な認証手法を検討してきた [3][4]．本論文では，これまでに提案した手法を基に、モバイルアドホックネットワークにおける認証モデルとその実現方法を議論する．また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ことにより，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．

3. 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．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ものとする．この環境において以下の 3 種類の認証手法を提案する．

認証手法 1 では互いに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，A は元から知っていた B の公開鍵を用いて認証する．この手法では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．認証手法 2 と 3 では公開鍵を知らないメンバが居合わせる場合を考える．認証手法 2 において，A は MANET 内で公開鍵を知る第三者であるノード T を探し B の公開鍵を教えてもらうことによって，B の認証を行う．この手法では T と B が共謀すれば不正を行えるためセキュリティレベルが低い．認証手法 3 では A が T の公開鍵を知っていた場合を考える．この手法では，A が T の公開鍵を用いて T を認証し，T が正しいと確認してから B の認証を行うのでセキュリティレベルが高い．ただし，以上の議論においては，正しい公開鍵で認証されたノードは不正を行わず，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. 認証手法の階層型認証機構への適用

4.1 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．

まず全てのノードはオープンなピアグループに属し，また各ノードは属する会員サービスの種類によって異なる ID をもっている．この ID を申告しあうことによって MANET 内でピアグループを形成し，通信を始める．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格納して，公開鍵リストを作成することができる．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，そのメンバと公開鍵に関する情報をピアグループ内で保有する．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，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．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 1 が A の持つリストであると考えると，B が ID を申告してきた際にはまず低レベル層に B の ID を追加する．この時，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場合には中レベル層に 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場合には認証手法 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．

会員サービス内の個々のメンバがそれぞれ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

Proposal and Implementation of Authentication System with Public Key Cryptosystem
† Naoko Ohara, Masato Oguchi
Department of Information Sciences, Ochanomizu University

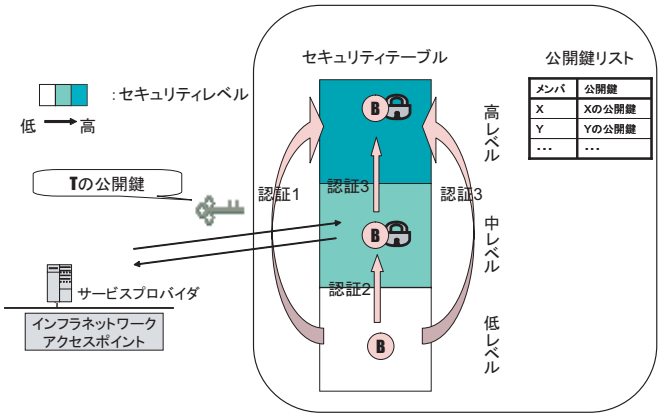

図 1: 階層型認証機構の提案モデル

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相手を高レベルに認定した際には，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．その際,A が B のテーブルのみに存在するノードを発見した場合には，そのノードと公開鍵を自分のテーブルに追加する．また，A が自分と B の両方のテーブルに存在するノードを発見し，かつ B のセキュリティテーブルの方がそのノードを高いレベルに認定していたら A はそのレベルにノードを更新する．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．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．

4.2 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 A が B を認証する際のアルゴリズムを以下に示す．

[認証に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して自分のセキュリティテーブルを更新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．

[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．

4.3 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 を JXTA 上に実装した．プログラムの受信側と送信側の実行結果を図 8 に示す．初めに受信側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]．以上のように，P2P 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．

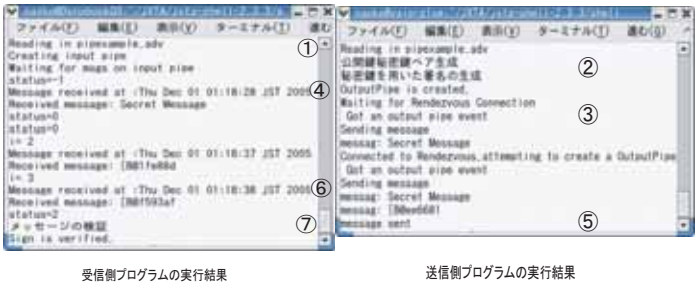

図 2: 認証手法 1 の JXTA 上のプログラム実行結果

5. 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，公開鍵暗号方式を用いてセキュリティレベルの異なる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，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．

参考文献

[1] http://www.jxta.org/docs/JxtaProgGuide_v2.3.pdf

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

[3] 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 67 回 全国大会，2T-8,2005 年 3 月

[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