アドホックネットワークにおける機器間の新しい信頼関係 ――機能に基づく認証方式の提案――

Karim Hamzaoui† 河口 信夫‡†

†名古屋大学大学院情報科学研究科
‡名古屋大学情報連携基盤センター

An Inter-device Trust Model for Adhoc Networks –Function-based Authentication–

Karim Hamzaoui † Nobuo Kawaguchi ‡†

†Graduate School of Information Science, Nagoya University
‡Information Technology Center, Nagoya University

1 はじめに

近年、計算機の小型化、携帯電話や PDA などの無線端末の普及にともない、コンピュータがあらゆる場所に存在するユビキタスコンピューティングが注目を集めている。ユビキタス情報環境の利便性は多様な機器やサービスの登場によって次第に高まりつつある。その一方で、セキュリティに関する課題も同時に増大しつつある。インターネットにおいては、セキュリティのインフラとして PKI（Public Key Infrastructure）が広く用いられており、公開鍵暗号化方式や電子署名に基づいたユーザ認証が情報セキュリティシステムの基盤となっている。これに対して、インターネットに接続されていない環境において携帯端末間で一時的に構築されるアドホックネットワークでは、PKI も、信用できる第三者も存在しないため一般的な認証システムの実現は困難である。しかしながらアドホック環境においても、機器間に何らかの信頼関係が存在すれば、信頼関係に応じたデータの通信が可能になる。

以下では、まず 2 節においてアドホックネットワークおけるセキュリティについて説明する。3 節では、機器間の信頼関係を新しく定義する。4 節では、機器上のソフトウェアが持つ機能に基づく認証方式を提案する。最後に本手法の実現可能性を検証するために、画像データを転送するプログラムの機能を JAVA の JDI に基づき実現したプロトタイプを紹介する。

2 アドホックネットワークにおけるセキュリティ

2.1 アドホックネットワークの特徴と問題点

通信ネットワークにおいて、ネットワーク上でやり取りされている電子データの完全性を保つことやユーザのプライバシーに関わる情報を扱ったサービスを安全に運用することは重要な課題となっている。必要に応じて構築されるアドホックネットワークにおいてもセキュアな通信が求められている。以下では、アドホックネットワークの特徴とそのセキュリティ上の問題点を挙げる。

- 無線通信によって構成されるため、固定ネットワークと比較して、通信データの盗聴や改ざんやなりすましなどの攻撃を受ける危険性が高い。
- セキュリティインフラ（PKI）が存在しない、あるいは、認証局に常にアクセスできない場合があるため、通信データの秘密性や完全性を保つための公開鍵暗号や電子署名が利用できない。

2.2 従来手法

前節で述べたセキュリティ問題を解決するために、インターネットで使われている認証モデル（階層モデルや PGP[1] の”web of trust”）をアドホックネットワークに使用する手法が提案されている。以下では、その中から主な二つを紹介し、現実のアドホックネットワークでの有効性について述べる。

Threshold cryptography:

[2] と [3] 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。この手法により、ネットワークの初期設定以外には信頼できる集中的な第三者がなくても証明書の発行や公開鍵暗号方式などのサービスを利用することができるようになる。しかしこの手法では、悪意を持つノードが偽の“ secret share ”を作ることによって自由に証明書を発行し、ほかのノードに対して攻撃する“ Sybil Attack ”[6] を避けることができない。また、N 台のノードが集まらないと認証

ができないため、ノード間の通信が切れることがあるアドホックネットワークでは安定した認証ができなくなる。

Secure side channel:

[4] と [5] では、電子データのやり取りを行いたい携帯端末が赤外線や有線などの短距離の物理的な接続が可能になる距離まで移動し、お互いの ID と公開鍵をバインドした証明書を交換するという仕組みが提案されている。短距離の接続ができないノードの認証情報を得るためには信頼できるノードによる中継が用いられる。

これらの手法では、インターネットで使われているユーザの ID 認証に基づいた信頼モデルが実現されている。これにより、第三者による攻撃が回避でき、相手とのデータ交換を安全に行える。しかし、アドホックネットワークにおいては、データを相手に安全に渡すだけではなく、そのデータを正しく利用してくれることを保証できる手段も求められる。例えば、個人の写真や名刺を送る場合、無制限にコピーされないようにデータを送りたいという要求がある。本研究では、この目的のために新しい信頼モデルについて検討する。

3 アドホックネットワークにおける信頼モデル

“ 信頼 ”という言葉は、さまざまな状況によって異なった定義で用いられる。人間社会においては、「正しい住民票を持っている」や「友達の紹介である」、「特定の組織に属している」などの事実に基づいて信頼関係が構築されている。インターネットにおいては、PKI を用いた認証情報、信頼できる第三者による推薦、計算機の属するドメインなどの情報に基づいた信頼モデルが用いられている。これらの信頼モデルでは、得られた情報から、何らかの手段によって通信における責任の所在を確認できる点が重要である。一方、アドホックネットワークにおいて、互いに共通の情報を持たない端末間では、責任の所在を確認する手段が存在しない。すなわち、アドホックネットワークでは人間社会やインターネット上と同じような信頼モデルを適用することが不可能である。アドホックネットワークにおいては、端末 ID はただの一時的な情報であり、端末の責任の所在については何も保証していない。このような匿名な環境において、初めてあったユーザとデータの交換を行いたい場合に、どのような信頼関係を築けるかをまず検討する必要がある。例えば、ネットワークゲームについて考える。ゲームに参加したいユーザは各自の携帯端末を利用して一時的な無線アドホックネットワークを構築する。この状況では、参加者にとっての心配は、他のユーザがゲームソフトウェアを改ざんして不当な参加をしているかどうかである。つまり、そのゲームの提供者の意図に沿ったソフトウェアを実行しているユーザに限って、信頼されてゲームへの参加を許可されるという仕組みが求められる。本研究では、あるユーザが「期待通りの振る舞いを取っている」という事が確認できれば、その振る舞いについてはユーザを信頼するという新しい信頼関係を定義する。すなわち、通信相手が受け取ったデータを正しく利用することを保証できれば、その点においてのみは相手を信頼するというモデルである。本稿では、この信頼モデルを「機能に基づく信頼モデル」と呼び、この信頼モデルによる端末間の認証を「機能に基づく認証」と呼ぶ。機能に基づく認証が行えれば、通信相手が誰であろうとも、データに対しては期待通りの振る舞いしか行わないためアドホックネットワークにおいても安心してデータ通信を行うことができる。

4 機能に基づく認証方式

4.1 アプローチ

本節では、「機能に基づく認証」を実現する手法について述べる。本稿では、シンプルな実現法として、自端末と相手端末が同じプログラムを動作されていることを確認することによって機能認証を実現するアプローチをとる。本アプローチでは、以下の項目を特徴とする。

- 機能の所有確認：初めて出会ったユーザとデータ通信をはじめる前に、相手が特定の機能を持っているどうかを確認する。
- 自己参照可能なバイナリコードの利用：相手端末上で動作しているプログラムが実行中のコードの任意のメモリ状態を確認する。
- 通信と認証を区別しない：相手に送りたいデータと認証用のデータを分けずに通信する。
- チャレンジレスポンス方式の使用：通信相手とデータを交換している最中に、相手端末上で実際に動作しているコードに対してチャレンジを送る。ここでは、“ Replay Attack ”のような攻撃の回避できるために、チャレンジをランダム的に変えていく必要がある。

4.2 機能認証コードの構成

機能に基づく認証を行うプログラムを機能認証コードと呼ぶ。機能認証コードは図 1 のように通信管理部と機能動作部から構成されている。

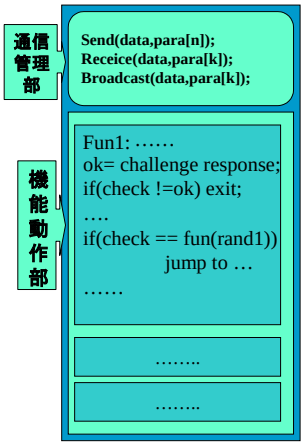

図 1: 機能認証コードの構成

通信管理部は、他の端末との通信と、通信相手の端末で動作しているコードの認証用のデータのやり取りを管理している部分である。そのため、send や receive や broadcast などのような関数が定義されている。通信管理部は、全ての機能認証コードに共通である。

機能動作部は、サービスの提供者の意図に沿った機能のコードが並べて記述されている。

4.3 機能認証の手続き

初めて出会ったユーザと通信したい時に、まず、相手がどんな機能を持っているを調べて、利用可能な機能認証コードを確認する必要がある。共通な機能の存在により、初めて相手とデータ通信が行える。以下では、機能認証コードの選択と機能の認証のそれぞれの手順を述べる。

- 機能認証コードを選択する段階：(端末間で行う)
  1. 端末が持っている認証コードの名称とそのハッシュ値の組をリスト化して通信相手に送る。
  2. 認証コードのリストから共通な認証コードを取り出す。
  3. 共通のコードのリストから実行したい機能を含んだ認証コードを選択し、実行する。

ここまでで、認証を行う対象のコードが選択された。通信相手がそのコードに定義している機能を使っている限りは、信頼できてデータのやり取りを安全にできると考えられる。次に、通信相手が改ざんされた機能を使っていないことの確認をチャレンジレスポンスの形で行う。以下の図 2 は、機能の認証手順を表している。

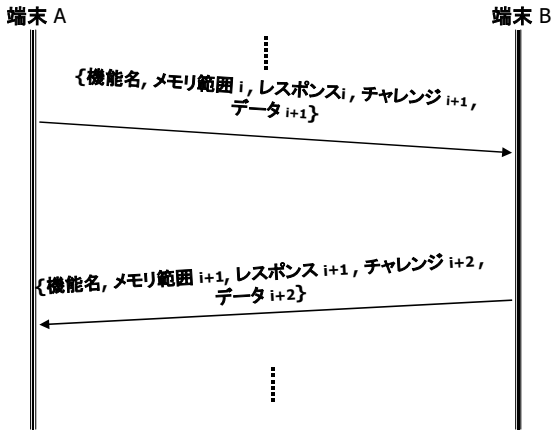

図 2: 機能認証の手続き

- 機能の認証：(認証コード間で行う)

  端末 A と端末 B は互いにチャレンジとレスポンスの交換を続けることにより、常に確認を行ない続ける。以下では、端末 B が端末 A からパケットを受け取った場合の処理を説明する。

  1. 相手の確認：端末 B は端末 A から受け取ったレスポンスを調べて、端末 A の実行しているコードが正しいことを確認すると同時にデータが改ざんされていないことを確認する。
  2. 受信データの復号化：指定されたメモリ範囲のコードを参照して、受信データを復号化する。
  3. 機能の実行：復号化したデータを用いて指定された機能を実行する。
  4. 送信データの暗号化：新たに任意のメモリ範囲を定め、そのコードを参照して、送信したいデータを暗号化する。
  5. チャレンジ・レスポンスの生成：受け取ったチャレンジに対するレスポンスを作成すると同時に次のチャレンジを生成する。
  6. パケットの送信：端末 A が実行すべき機能、メモリ範囲、レスポンス、チャレンジ、データをパケットにして送信する

5 考察

5.1 アドホックネットワークへの適用

3 節で述べたように、アドホックネットワークにおいてはノードの ID のような認証情報に基づいた信頼モデルでは、責任の所在が確認できない。それに対して、本研究で提案した手法では機器の振る舞いに基づいて信頼関係を構築することができる。また、機能認証を端末間で直接行うためセキュリティインフラのサーバや信頼できる第三者に依存せずに判断が可能となる。

5.2 各種攻撃への対応

本手法を用いることによって、以下に述べる第三者による攻撃を回避できる。

通信データの盗聴 (Eavesdropping)：アドホックネットワークは基本的に無線通信によって構築されるため、通信データとパケットの読み取り、監視を簡単に行うことができる。本手法では、メモリ上のコードを用いて通信データを暗号化する。そのため、同じ機能を持っていない第三者がデータを盗聴しても復号化を行えないのでデータの利用ができない。また、やり取りのデータとチャレンジレスポンス用のデータをわけずに通信を行うことによって、それを分析できるコードを持っていない端末はデータだけの盗聴が不可能である。本稿では、機能認証コードの配布方法によって二つの種類に分ける：

- 公開認証コード：ネットワーク上で配布されているデータを全ての端末が受け取れるように、用いられる認証コードを事前に配布したり、公開する。このような場合では、配布するデータに対して提供者の意図に沿った利用が保証できる。
- 非公開認証コード：電子データを特定な相手、あるいは、グループメンバーにしかデータを受け取れないようにしたい時に、用いられる認証コードを安全な通信で配布する必要がある。

通信データの改ざん (Alteration)：アドホックネットワークでは、直接通信ができない機器間は中継ノードを経由して通

信するので、悪意のある中継ノードが通ってきたデータを読み取った後に、改ざんしてからもう一回受信側の機器に送ることが可能である。本手法では、信頼できる機能の処理の一部としてチャレンジに対するレスポンスも同時に計算すると前提する。そうすると、データを受け取る側では、チャレンジのレスポンスを調べることによってデータが途中で改ざんされたかどうかを確認できる。

なりすまし攻撃（Spoofing）：本研究では、ユーザの認証情報を用いていないため、本質的になりすまし攻撃は不可能である。

反射攻撃 (Replay attack): 本手法では、機能を実行するたびに、対象の両方の機器がランダム数を生成してそのセッションの一つのパラメータとして使われている。また、チャレンジの内容が毎回変わるので、ある通信セッションのパケットは他のセッションで利用できない。

6 実装プロトタイプ

本手法の実現可能性を検証するために、画像データを転送するプログラムの機能を JAVA で実現した。ここでは、受信ユーザが受け取ったデータ画像を 10 秒しか見れないという機能の認証を実現するのが目的である。そのために、本プロトタイプでは、VM 上で実行しているクラスやメソッド などの実行状態を調べることができる JAVA の JDI[7] を用いて、相手端末上で実行されているコードを確認することが可能になる。また、動作している機能のクラスのハッシュ値を利用して転送したい画像データを変換することによって、同じ機能を実行している端末しか元の画像データに戻すことができない。以下の図 3 では、プログラムの実行結果の例を表している。ここでは、正確な機能を実行している HostA と HostB と受け取った画像を無制限に見れるようにした改ざんの機能を実行している HostC について考える。通信データの盗聴攻撃に対する回避を確認するために、チャレンジレスポンスに失敗した端末に対してもデータを送ることにした。図で見て分かるように、HostB が正確な機能を実行しているので受け取ったデータを元の画像に戻すことができた。それに対して、悪意を持つ HostC は改ざんされた機能を実行しているので、データを受け取っても画像を見れない状態を確認できる。

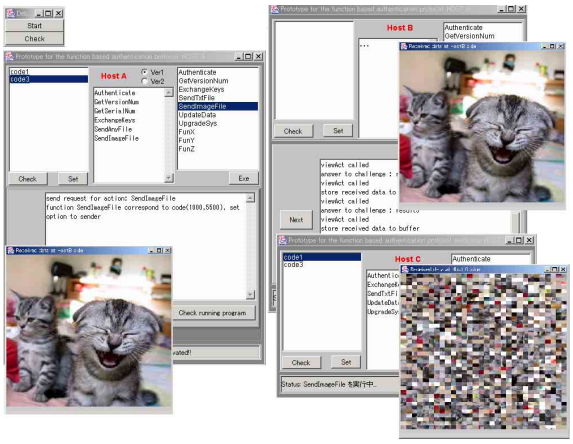

図 3: プロトタイプの実行結果

7 まとめ

本稿では、アドホックネットワークにおけるセキュリティ課題に対して、機能に基づく認証方式を提案した。また、アドホックネットワークに適応した信頼関係を定義し、セキュリティシステム基盤が存在しないネットワーク上でも同一の機能を持つ機器間で安全な情報通信の可能になった。機能に基づく実装も、JAVA の JDI を利用したプロトタイプを作成し、本手法の実現可能性を確認した。今後は、マシンコードレベルでの機能認証の実装と機能認証コードの作成支援について検証する予定である。また、端末間だけではなく、モバイルエージェント間の機能の認証を検討した上で、我々開発しているモバイルエージェントミドルウェア Cogma[8] での実現が今後の課題として考えている。

謝辞

本研究の一部は平成 15 年度産業技術研究助成事業事業費助成金（「安全なユビキタス社会を実現する組み込み機器用アドホックネット基盤ソフト」）からの支援を受けて行ったものである。ここに記して謝意を表す。

参考文献

[1] Alfarez Abdul-Rahman The PGP Trust Model , EDI-Forum: The Journal of Electronic Commerce (1997)

[2] L.Zhou and Z.Haas：Securing ad hoc networks, IEEE Networks, 13(6):24-30 (1999)

[3] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang：Self-securing Ad Hoc Wireless Networks, IEEE Symposium on Computers and Communications (2002)

[4] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan：Self-Organized Public-Key Management for Mobile Ad Hoc Networks , IEEE Transactions on Mobile Computing, (2003).

[5] D. Balfanz, D. Smetters, P. Stewart, and H. Wong：Talking to strangers: Authentication in ad hoc wireless networks, In Proceedings of the 9th Annual Network and Distributed System Security Symposium (NDSS), (2002)

[6] J. Douceur： The Sybil attack, In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (PTPS), (2002)

[7] JDI(Java Debug Interface)：(http://java.sun.com/j2se/1.3/docs/guide/jpda/jdi/)

[8] 河口信夫, 稲垣康善：cogma:動的ネットワーク環境における組み込み機器間の連携用ミドルウェア, 情報処理学会コンピュータシステム・シンポジウム, pp.1-8 (2001).