無線可視領域ネットワークにおける端末相互認証手法

野田, 厚志
九州大学大学院システム情報科学府情報工学専攻 : 博士後期課程

阿瀬川, 稔
九州大学大学院システム情報科学府情報工学専攻 : 修士課程

北須賀, 輝明
熊本大学大学院自然科学研究科

田頭, 茂明
九州大学大学院システム情報科学研究院情報知能工学部門

他

https://doi.org/10.15017/1517964

出版情報 : 九州大学大学院システム情報科学紀要. 14 (2), pp.77-82, 2009-09-25. Faculty of Information Science and Electrical Engineering, Kyushu University
バージョン :
権利関係 :

九州大学大学院
システム情報科学紀要
第14巻 第2号 平成21年9月

Research Reports on Information Science and
Electrical Engineering of Kyushu University
Vol.14, No.2, September 2009

無線可視領域ネットワークにおける端末相互認証手法

野田 厚志* ・ 阿瀬川 稔** ・ 北須賀 輝明*** ・ 田頭 茂明†
北口 貴史†† ・ 津村 直樹†† ・ 中西 恒夫† ・ 福田 晃†

A Mutual Authentication Method on Wireless Visible Area Network

Atsushi NODA, Minoru ASEGAWA, Teruaki KITASUKA,
Shigeaki TAGASHIRA, Takashi KITAGUCHI, Naoki TSUMURA,
Tsuneo NAKANISHI and Akira FUKUDA

(Received June 12, 2009)

Abstract: A spread of mobile terminal equipped with short-range wireless communication device has increased the demand for file sharing through local and temporary wireless network. However, due to the ease of sniffing in such network, the file sharing has a risk of leaking in the communication. In this paper, we focus on secure face-to-face information exchange especially in wireless visible area network (WVAC) which is locally and temporarily constructed to communicate with visible users. More concretely, we propose a mutual authentication method for WVAC. The proposed method enables a communication pair to mutually authenticate their public keys without any certificate authority. The main idea of the proposed method is to authenticate the public keys of the communication pair based on trusting relationship obtained by a face-to-face situation. Additionally, users obviously can comprehend authenticated public keys for others due to man-in-the-loop approach included in the process of the authentication.

Keywords: Wireless communication, Wireless visible area network, Mutual authentication, File sharing, Local and temporary wireless network

1. ま え が き

先進的なユーザは持ちよった端末間で無線通信でのファイル共有を行える環境にある．ノートPCへの無線LAN搭載が標準的であり，携帯電話の一部でもBluetoothや無線LANが搭載されている．近距離無線通信機能は，インターネットアクセスなどの位置透過型の通信には不向きな面も多いが，携帯電話とヘッドセット間のPAN (Personal Area Netowrk)での利用が進んでいる．筆者らは近距離無線通信機能が今後，対面している利用者の端末間での通信に盛んに利用されるようになることを想定している．たとえば，営業担当者が企業を訪問した際に電子的な資料を無線通信で手渡したり，喫茶店で友人同士がデジカメの画像をやり取りしたりする状況である．このような状況において，現時点ではUSBメモリなどの物理媒体や，電子メールなどのインターネット通信を利用したファイル交換が盛んであるが，無線通信機能を利用したファイル交換が行われることは比較的少ない．無線通信機能をより直感的かつ信頼して利用できるようにすることで，その一部は利用者同士が対面している状況を活用した近距離無線通信に置き換わっていくことが推測される．

無線通信に対する信頼の低さのひとつとして，盗聴などの攻撃に対する安全性への不安があげられる．事実，安易に構成された無線ネットワークは盗聴が比較的容易であり，共有するファイルなどが不用意に漏洩する危険性を伴う．また誤った相手への送信などの事故による漏洩も心配の一因である．現在でも一定の知識と労力を伴えば安全なネットワークを構築することができるが，情報工学や計算機科学の専門家であってさえ，労力を払うより，より確実で慣れ親しんだ物理媒体やインターネット通信を好む傾向にあり，非専門家はその多くが利用しない状況にある．

本論文で想定する無線可視領域ネットワークとは，利用者の携帯端末と目前の第三者の端末とで構成される無線ネットワークである．第三者の端末としては，目の前にいる人物の端末や，インターネットキオスクなどに設置されたプリンタなどの公共機器を想定している．PANとは異なり，ネットワーク内の端末の一部は，利用者自身の所有ではなく，利用者の周囲の見える範囲にある端末である．複数人で構成する点を除いてPANに近い近距離端末間の通信を想定している．この無線ネット

平成21年6月12日受付
* 情報工学専攻博士後期課程
** 情報工学専攻修士課程
*** 熊本大学大学院自然科学研究科
† 情報知能工学部門
†† 株式会社リコー

ワークは，無線LANでいえばアドホックモードでのpeer-to-peer通信で構成されるネットワークであり，アクセスポイント等のインフラやインターネット接続性は必ずしも必要とせず，その代わり通信相手の端末（もしくは端末利用者）が見える範囲にいることを前提とするネットワークである．無線ネットワークの構成に依存するものではないが，盛んに研究されているマルチホップの無線アドホックネットワークよりむしろ，シングルホップの無線ネットワークを想定している．

本論文では，この無線可視領域ネットワーク上で端末を相互に認証する手法の提案と開発について述べる．本手法は認証局を用いずに相互に端末を認証し，互いに認証した端末間で暗号化を行ったファイル共有を実現し，主に中間者攻撃と誤った端末への送信を防ぐ効果を持つ．端末の相互認証には公開鍵暗号を用いるが，互いに対面する利用者間の信頼関係をよりどころとして，利用者が互いの端末の公開鍵を確認しあうことで，相互認証を実現する．認証手順の中に人間の確認作業を含めるman-in-the-loopアプローチによって，利用者自身が認証の有無を明らかに認識することができるため，誤った端末への送信が防がれる．

本論文の構成は以下の通りである．第2章では公開鍵認証に関する技術を紹介し，無線可視領域ネットワークに適用した場合に生じる課題について示す．第3章では本論文で提案する手法についての解説を行う．第4章で提案手法の実装と，実験的な評価について記述する．また提案手法の各種攻撃に対する耐性について考察し，第5章でまとめと今後の課題について示す．

2. 関 連 研 究

公開鍵暗号を用いて安全な暗号化通信を実現するためには，公開鍵の認証を正しく行う仕組みが必要である．公開鍵を認証する仕組みとして公開鍵基盤(PKI; Public Key Infrastructure) がある．公開鍵基盤とは，公開鍵を効率的に運用するために定められた規格や仕様の総称である．信頼できる第三者機関に公開鍵の証明書を発行してもらうことによって公開鍵の認証を行う．本研究で対象としている環境においては，認証局が存在するネットワークに接続していない場合も想定するため，公開鍵基盤を利用した公開鍵認証を利用できるとは限らない．認証局を利用せずに，利用者間の信頼関係を利用することによって公開鍵の認証を実現する仕組みとして，Web of Trust（信頼の網）がある．Web of Trustを利用する具体的な例としては，PGP[1]がある．Web of Trustをベースにした公開鍵認証では，事前に利用者間の信頼関係が構築されている必要がある．本研究で対象とする環境においては，初対面の利用者間での利用も想定しているため，Web of Trustを利用した公開鍵認証を利用することができない．

第三者を利用せずに当事者間で公開鍵を認証する仕組みが提案されている．基本的なアイデアは，公開鍵の指紋（Finger Print）と呼ばれるハッシュ値の一致性を何らかの手段を用いて確認することである．この指紋を確認する手段として，確認を容易にし，間違いを判別しやすくするために，文献 2)では，文字列，図画，および可聴音を用いることが提案されている．また文献 3) では，当事者が発話する音声を用いて一致性を確認することが提案されている．具体的には，指紋の1バイト毎に英単語を割り当て，利用者が発話し易いように指紋の表現形式を変換している．この変換に用いる英単語のリストのことをBiometric Word Lists と定義している．Biometric Word Listsに含まれる英単語には発音の違いや，識別のしやすさ，言いやすさなどを基準にして選出された英単語が採用されている．このBiometric Word Listsは，音声通信を用いて公開鍵の認証を行う際に用いる英単語のリストのことである．元々PGPfone(Pretty Good Privacy Phone) [4]での公開鍵の認証のために設計，実装された．Biometric Word Listsを用いた公開鍵の認証では，インターネット電話などの音声通信上で口頭による英単語の照合を行う．しかし，利用者同士が相互に公開鍵の認証を行う場合には，英単語の照合を双方向に行う必要があり，利用者への負担が大きくなるという欠点がある．

3. 提 案 手 法

本章では，無線可視領域ネットワークにおいて，公開鍵の認証を容易に行うための手法として，二者間での認証に着目し，「表形式確認方式」を提案する．具体的には，提案手法は2.章で説明した公開鍵の指紋の一致性を確認することをベースにしており，その指紋の表現方法において視覚情報を用いることで，確認を容易にすることを図っている．視覚情報として，英単語表を利用する．利用者が対面していることを利用し，口頭または目視によって視覚化された情報を確認することによって公開鍵の認証を行う．また，利用者の公開鍵の認証を一度で相互に行うことができる利点を持つ．

本論文では，利用者間での暗号化通信の開始を指示した利用者をホスト，ホストから暗号化通信の開始の指示を受けた利用者をゲストと定義し，各々が所持する無線端末をホスト端末，ゲスト端末と呼ぶ．

次節以降，提案手法の詳細について説明する．

3.1 表形式確認方式

表形式確認方式では，視覚情報として英単語表を用い，同一性を確認することによって公開鍵の認証を行う．まず表形式確認方式で用いるサマリの定義と乱数について述べ，その後表形式確認方式での公開鍵の認証の流れと

有用性について述べる．

3.1.1 サマリ

サマリとは，データのハッシュ値のことであり，表形式確認方式ではハッシュ値は英単語表に一意に変換される．サマリs_1は自身の公開鍵k_A，自身が生成する乱数r_A，相手の公開鍵k_B，相手が生成する乱数r_Bから生成される．ハッシュ関数を$h()$とすると，以下の式でサマリs_1を求める．

$$s_1 = h(k_A, r_A, k_B, r_B)$$

乱数とは，それぞれの利用者によって生成される数値のことであり，認証開始時にそれぞれ生成し，相手へ送信する．サマリの生成と英単語表への変換は以下の手順で行われる．

1. $h(k_A, r_A, k_B, r_B)$を計算し，サマリs_1を得る
2. サマリs_1を分割
3. 分割した値を基に，英単語表に表示する英単語を選択

サマリを生成する基になるデータをハッシュ関数に入力すると，出力としてサマリが一意に決まる．もし入力したデータのうち1ビットでも異なれば，異なるサマリが生成される．英単語表もまたサマリに対して一意に決まるので，英単語表の同一性を確認することはつまり，サマリが同値であることを確認することと同意である．

端末間でのデータ交換が正常に行われたと仮定すれば，正当な公開鍵と乱数から生成されたサマリは，ホストとゲストの間で同値になる．自身の端末と相手の端末の画面に表示されている英単語表が異なる場合には，サマリを生成する基となるデータk_A，r_A，k_B，r_Bのうち，自身に関するデータk_A，r_Aは間違いなく正当なものであるので，受信したデータk_B，r_Bのいずれかが不正なデータであることを示唆している．

お互いの端末に表示されている英単語表が同一である場合，サマリ生成の基のデータが完全に一致していることから，相手と全く同じデータを共有していることになり，受け取った公開鍵が相手が持っている公開鍵と同一の鍵であると判断することができ，認証が完了する．対面する相手とは信頼関係にあるため，その公開鍵に対応する秘密鍵を持ち，暗号化されたデータを復号化することができるのは対面する相手のみである．

英単語表の同一性を確認する方法としては，英単語を全てまたは指定したセルの英単語を読み上げることによって口頭で確認する方法，あるいはお互いの端末を並べて画面に表示英単語表を比較することによって目視で確認する方法が考えられる．

公開鍵のハッシュ値を英単語に変換し，利用者自身が英単語を確認する点においては，2.章で紹介した

	1	2	3	4
1	friend	million	law	he
2	president	absent	remember	open
3	college	eye	class	police
4	kiss	pie	frog	rock

Fig. 1 Output image for summary confirmation table.

Fig. 2 Output image for summary confirmation table with font and color.

Biometric Word Listsと同様であるが，音声以外の視覚情報も英単語の確認方法として用いることができるという想定環境に違いがある．また，Biometric Word Listsでは1度の認証手順で一方の利用者の公開鍵しか認証できないが，本手法では1度の認証手順で双方の利用者の公開鍵の認証が可能となっている．加えて，本手法では英単語表のフォントや色を変えることにより，表サイズを小さくすることができ，さらに効果的に同一性を確認することができる．

4. 評　　価

本章では提案手法の実装について述べ，提案手法の評価を行う．評価は，サマリ確認に要する時間と誤答数に関して，提案手法と従来手法とを比較する．また，表のサイズの縮小や，定性的な評価を行い提案手法の各攻撃に対する耐性について考察を行う．

4.1 提案手法の実装

提案手法の実装を行った．今回は，利用者の所持している無線端末の位置情報を利用したメッセンジャーアプリケーションLAIM(Location Aware Instant Messenger)[5]に提案手法による認証機能を追加し，暗号化してメッセージを交換できるアプリケーションに拡張した．LAIMでは携帯端末の相対位置を把握することができ，利用者は画面上に表示されている利用者とメッセンジャー機能を利用してコミュニケーションを行うことができる．メッセージの暗号化の手順としては，（1）まず利用者間で公開鍵を交換する．（2）提案手法を用いてその公開鍵の認証し，正しければ公開鍵を用いて，共通鍵を交換する．（3）以降，その共通鍵を用いてメッセー

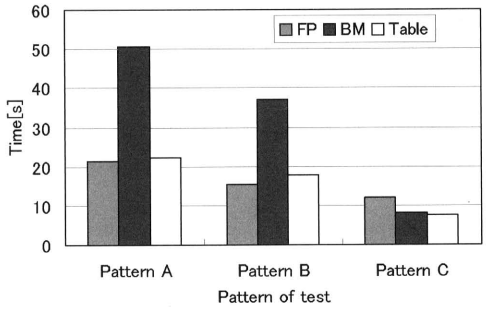

Fig. 3　Time required fororal confirmation.

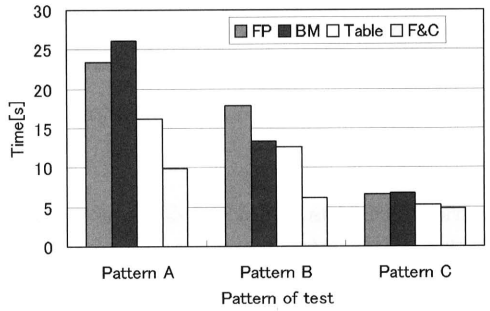

Fig. 4　Time required forvisual confirmation.

ジを暗号する．公開鍵の鍵ペアについては各々の携帯端末内で既に生成されているものとし，公開鍵および秘密鍵の鍵長は2048ビットとした．また，サマリおよび短いサマリの生成に用いるハッシュ関数にはSHA-1関数[6]を利用した．

サマリを生成する基になるデータはホストの公開鍵k_H，ホストの乱数r_H，ゲストの公開鍵k_G，ゲストの乱数r_Gから成り，それぞれ，2048ビット，16ビット，2048ビット，16ビットとした．基になるデータをSHA-1関数に入力し，出力である160ビットのハッシュ値をサマリとして利用する．サマリを最上位ビットから10ビット毎に分割し，10ビットで表現される数値から，あらかじめ準備しておいた英単語のリストから単語を1つ選択し，英単語表の対応するマスにセットする．表形式確認方式で用いる英単語のリストは1024語の英単語から成り，10ビットで表現される1024通りの数値にそれぞれ対応している．ここでの英単語は，辞書から簡単な単語を無作為に抽出し，よく似た単語は削除したものを利用している．160ビットを10ビット毎に英単語にするため，生成される表のサイズは，4×4の16マスとなる．また，フォントと色を用いた表形式確認方式では，フォントに4ビット，色に4ビット，残りを英単語に割り当てた．この場合，3×3の英単語表になる．

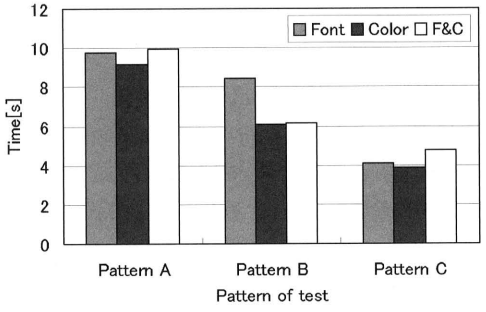

Fig. 5　Impact of font and colorinformation.

4.2　実験環境

提案手法の評価を実験を通して行った．実験用に，既存手法と提案手法によるサマリを連続して出力するソフトウェアをPC上に実装し，利用者にサマリの確認をしてもらい，確認に要する時間と誤答数を評価項目として計測した．実験は，2台の同一のノートPCを用いて行った．2台のノートPC上に表示されるサマリが同一のものであるか口頭・目視により確認する．口頭による確認では，ふたりの利用者がそれぞれ1台のノートPCを利用して，ノートPC上に表示されるサマリを口頭により確認する．目視による確認では，ひとりの利用者が同時に2台のノートPCを利用して，2つの画面上に表示されるサマリを目視により確認する．

本実験で用いたサマリの表現形式としては，指紋方式(16進数)，Biometric Wordを4 × 4の表形式で出力した方式，表形式確認方式，表形式確認方式（フォント変更），表形式確認方式（色変更），表形式確認方式（フォントと色を変更）の計6種類である．ただし，口頭による確認の場合は，フォントまたは色を変更する表形式確認方式を除く計4種類とした．**Fig.1**，**Fig.2**に，表形式確認方式，表形式確認方式（フォントと色を変更）の出力例を示す．

実験に用いる問題として，2つのサマリが同一の問題（Pattern A），一方のサマリ内にひとつの単語（指紋の場合は文字）だけ誤りを含ませた問題（Pattern B），一方のサマリ内に半分誤りを含ませた問題（Pattern C）を用意した．また，誤りを含ませる箇所はランダムとしている．合計問題数を60問とし，その内訳は，口頭による確認のために，4種類の表現形式ごとに，Pattern Aを3問，Pattern Bを2問，問題C を1問の計24問（= 4 × 6）を準備し，目視による確認のために，6 種類の表現形式ごとに，Pattern Aを3問，Pattern Bを2問，Pattern Cを1問の計36問（= 6 × 6）を用意した．この問題を3セット分用意し，その内1セットをランダムに選び，口頭での確認として10組，目視での確認として20人に対して実験を実施した．実験の被験者は日本人であり，情報工学を専攻する学生である．

4.3 実験結果

実験結果について説明する．**Fig.3**は，口頭での確認の結果である．横軸は問題パターンを示し，縦軸は確認に要した平均時間を示している．図中のFP は指紋方式，BMはBiometric Wordを用いた方式，Tableは表形式確認方式を指している．

結果からBMはPattern AとPattern Bに関して，確認に時間が必要であることがわかる．特に，Pattern Aに関しては50秒近く要している．これは利用される英単語が，発音の違いや，識別のしやすさ，言いやすさなどを基準にして選出されており，被験者が日本人であること，読めない英単語が出てきた場合ではアルファベットを読むことで確認していたこと，などが原因と考えられる．母国語を英語にしている被験者で実験をした場合には，異なる結果が得られたと思われる．BM におけるPattern Cの結果で，他の表現形式と比較して差がない理由は，Pattern Cは含まれる英単語の半分が誤りであり，確認過程の早期に誤りを発見できるためである．また，FPとTableの結果にあまり差がないことがわかる．これは，FPのように1次元で表示する場合と，Tableのように2次元（表形式）で表示する場合とでは，口頭で確認する限りは，その確認方法に差がないためだと考えられる．最後に，口頭での確認において誤って回答した問題はないという結果が得られた．口頭での確認は，正確に確認できると考えられる．

次に目視での確認の結果を**Fig.4**に示す．横軸と縦軸が示す値は，口頭での確認の結果と同じである．図中のF&Cは，表形式確認方式（フォントと色を変更）を指す．その他の凡例は口頭での確認の結果の場合と同様である．図の結果から，口頭での確認と比べて目視での確認の方が，FPを除いて短時間で確認出来ていることがわかる（FPは若干悪いか同程度である）．FPが改善しない理由は，FPのように16進数を単に表示した場合では，口頭または目視による確認方法が変わらないためだと考えられる（つまり，先頭から順番に確認していくことになる）．一方，BMやTableのように表形式で表示する方法では，口頭と比べて確認時間の改善がみられる．特に，BMはTableと同程度の確認時間を達成している．これは，表形式で表示することで目視による確認がし易いこと，またBMにおいて口頭による確認の問題だった読めない単語に関して，単なる文字列の比較で確認できること，などが理由として考えられる．一方，F&Cが，BMやTable以上に良い結果を得ていることがわかる．F&C は，Tableとの比較から，目視での確認において，フォントと色の情報が非常に有用であることを示している．最後に，目視での確認における誤答数について述べる．目視での確認において，BMで5回，Tableで2回の誤答があった．その他の方式では誤答はなかった．Tableの誤りは，同一であるのに同一でないという回答だった．一方，BMの誤りは，同一でないのに同一であるという回答が4回あり，現実的には非常に危険な誤りである．このことから，BM手法における安全性に関してさらなる考察が必要である．

次に，目視での確認においてF&Cが有用である結果に関して，フォントもしくは色のどちらの情報が有効なのかを実験により確認した．実験は，表形式確認方式（フォント変更），表形式確認方式（色変更），表形式確認方式（フォントと色を変更）の3種類の方式を用いて確認時間を比較した．結果を**Fig. 5**に示す．図中のFは表形式確認方式（フォント変更）を示し，Cは表形式確認方式（色変更）を示す．結果から，Cだけを用いた場合と，F&C の結果がほぼ同様になった．また，Fの結果はそれほど改善されていないのがわかる．これから，フォント情報よりも色情報が確認時間に影響を与えることがわかる．

4.4 表形式に関する考察

表の形に並べられた3方式（BM，Table，F&C）を比較した場合，実験により，BM，Table，F&Cの順に確認に時間を要するという結果が得られた．これは，確認する要素の数に起因するところが大きいと考えられる．

単純に要素数を減らすことにより，さらに確認時間を低減できるとも考えられるが，要素数を減らすためには，各要素の情報量を増やす必要がある．例えば，4×4のTable 形式の場合，16マスで160ビットを表現するため，各マスは10ビットの情報量となる．そのため，英単語を2^{10}（1024）通り準備している．しかしながら，表を3×3とした場合，要素数を9つに低減できるが，9マスで160ビットを表現するためには，各マスは18ビット，英単語にして2^{18}（262144）通り準備する必要がある．

また，英単語の代わりに図画を用いて視覚的認識を高めることも考えられるが，上記のような多数パターンの識別可能な画像を用意することは非常に困難である．

そこで，提案方式では，セキュリティ強度を維持しつつ，確認すべき要素数を減らすために，色とフォントに情報を持たせる工夫を行っており，色で4ビット，フォントで4ビットを表現することにより，要素数の低減と各マス目に用意すべき英単語数の抑制を両立している．

4.5 定性的評価

計算機ネットワーク上で想定される攻撃方法として総当たり攻撃，中間者攻撃，再生攻撃，類似攻撃の4つの攻撃方法について解説し，提案手法の各攻撃に対する耐性について考察を行う．

4.5.1 総当たり攻撃

総当たり攻撃とは暗号などに対して理論的にあり得るパターン全てを試すことにより解読を試みようとする方法である．公開鍵の認証手順に対する攻撃のみを対象と

し，公開鍵暗号に対する攻撃は今回は議論の対象としない．

表形式確認方式に対して考えられる攻撃方法としては，正規のサマリとサマリが一致する公開鍵を総当たりで発見し，このペアをホストやゲストに送信することが考えられる．しかし，提案手法では，認証毎に異なる乱数を用いるため，正規サマリと同値になる別の公開鍵を事前に用意することは困難である．認証時に即時に別の公開鍵を求めることは時間的制約から難しい．

4.5.2 中間者攻撃

中間者攻撃とは攻撃者がデータの送信者と受信者の間に入り込み，送信者に対しては受信者のように，受信者に対しては送信者のようになりすます攻撃である．提案手法の場合では攻撃者は，ホストに対してはゲストに，ゲストに対してはホストになりすます事が考えられる．しかし，提案手法では，なりすました別のホストから違う鍵を渡された場合，ホストとゲストの画面に表示されるサマリが異なり，認証が成功しないため，中間者攻撃が成功することはない．

4.5.3 再生攻撃

再生攻撃とは，攻撃者が通信を盗聴し，他の利用者同士によって行われた正規の認証での通信内容を記録しておき，同じ通信内容を再び利用することによって認証を成功させる攻撃方法である．

表形式確認方式では，認証中の通信で公開鍵と乱数がやりとりされるが，乱数は認証毎に異なるため，再び同じ乱数を用いない限り再生攻撃は成功しない．乱数はワンタイムパスワードと同様の役割を果たしている．仮に再生攻撃によって攻撃に成功したとしても，認証されるのは攻撃者の公開鍵ではないので，その公開鍵によって暗号化されたデータを攻撃者は復号化することができないので，再生攻撃は意味を成さない．

4.5.4 類似攻撃

類似攻撃(Similarity attack)とは人間の認識能力に対して働きかける攻撃方法である[7]．視覚的に類似するものを提示することにより，利用者に正規のものと勘違いさせ，誤った認証を行わせる事が目的の攻撃である．

表形式確認方式では，英単語表を生成する基となるデータが全てネットワーク上を流れるため，攻撃者は正規のサマリ，つまり正規の英単語表を推測することが可能である．したがって，攻撃者が正規の英単語表と類似した英単語表を生成可能な公開鍵と乱数のペアを準備できる可能性がある．攻撃者はその公開鍵と乱数を，認証に参加している利用者に送りつけることにより，英単語表が一致していると誤認させることができる恐れがある．

提案方式において，正規の英単語表における類似性が高いほど，利用者は誤認する確率が高くなると考えられる．類似攻撃による攻撃を成功させないためには，表示される英単語表をすべて確認することが効果的であると考えられる．

5. ま　と　め

本論文では，無線可視領域ネットワークにおける暗号化通信の重要性と，暗号化に関連する問題として，公開鍵の認証の必要性とその問題点について述べた．問題点を解決するために，利用者同士が近距離で対面していることを利用し，相互に公開鍵の認証を行うことのできる手法として，「表形式確認方式」を提案した．評価実験の結果，提案方式は従来方式よりも確認に要する時間が短いことがわかった．位置情報を利用する既存のアプリケーションに機能を追加する形で，提案方式の実装を行った結果，英単語表を用いてサマリの一致性を確認することにより，公開鍵の認証を行い，暗号化通信を開始ができることが確認できた．

今後の課題としては，認証済みの公開鍵を管理することによって，再び暗号化通信を開始する際の手間を軽減する仕組みや，グループの管理を行うことによって，利用者が複数のグループに所属しながら，グループに応じて平文・暗号文の使い分けができる仕組みを追加することが考えられる．

謝　辞

本研究の一部は(株)リコーと九州大学との共同研究契約に基づき行ったものである．

参 考 文 献

1) Atkins, D., Stallings, W., and Zimmermann, P.: PGP Message Exchange Formats, IETF RFC 1991 (1996).
2) 下遠野 享：対面無線アドホック通信に適した暗号通信路構築方法，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO）シンポジウム論文集，pp.559–562 (2002).
3) Juola, P., Zimmermann, P.: Whole-word phonetic distances and PGPfone alphabet, *Proc. Fourth international Conference on Spoken Language Processing*, Vol 1, pp.98–101 (1996).
4) Zimmermann, P.: PGPfone Owner's Manual (1996).
5) 片桐誉裕，野田厚志ほか：位置情報を使った近くの端末との直観的アドホック通信ソフトウェア，情報処理学会 第47回プログラミング・シンポジウム報告書，pp.199–202 (2006)．
6) Eastlake, D. 3rd, Jones, P.: US Secure Hash Algorithm 1 (SHA1), IETF RFC 3174 (2001).
7) Pering, T., Sundar, M., Light, J., and Want, R.: Photographic authentication through untrusted terminals, *Pervasive Computing, IEEE*, Vol.2, Issue 1, pp.30–36 (2003).