情報処理学会論文誌 Vol.53 No.5 1532–1545 (May 2012)

推薦論文

小型携帯端末のためのマルチパスの伝送路可逆性を用いた共有情報生成方式

岩本 智裕[1,a)] 田頭 茂明[2,b)] 荒川 豊[2,c)] 福田 晃[2,d)]

受付日 2011年7月1日, 採録日 2012年2月3日

概要：携帯電話やスマートフォンなどの小型無線端末の普及にともない，ユーザ同士が端末を持ち寄って一時的な無線ネットワークを形成し，互いにデータ通信を行う機会が今後ますます多くなることが予想される．このような近距離無線ネットワークにおいて，近くにいるユーザと安全かつ簡単にデータ交換を実現することは，近距離無線ネットワークの普及に必要な技術課題だと考える．本論文では，安全なデータ通信を実現する上で必要な共有情報（共通鍵）を，送受信端末で個別に生成する手法を提案する．提案手法の主なアイデアは，送信端末を振ることにより生じる無線伝送路の変動から共通鍵を生成することである．この無線伝送路の変動は，受信信号強度の同一の変動として観測され，この受信信号強度の変動から共通鍵を生成する．受信信号強度から生成される情報は，送受信端末間でのみ共有できる情報となる．さらに，提案システムを実装したプロトタイプシステムを構築し，提案手法の有効性を実環境において評価した．結果から，約 3 秒以内に 128 bit の共通鍵を 95%以上の精度で生成することをを確認した．

キーワード：伝送路可逆性，フェージング，近距離無線通信，共通鍵，堅牢性

A Generation Technique of Common Information Exploiting Characteristics of Multipath Fading Channel for Handheld Devices

Tomohiro Iwamoto[1,a)] Shigeaki Tagashira[2,b)] Yutaka Arakawa[2,c)] Akira Fukuda[2,d)]

Received: July 1, 2011, Accepted: February 3, 2012

Abstract: An explosive spread of handheld devices with wireless communication capability, such as cellular phone and smart phone, rapidly increases an opportunity for data communication through temporarily constructed short-range wireless networks. An easy realization of the secure data communication in such networks is indispensable to user-friendly networking environment towards the popularization of short-range wireless networks. In this paper, we propose a common key sharing technique which generates the encryption key on a communication pair rather than distributes a prepared key from one to the other. The main idea of the proposed technique is to generate a common key based on the variation of multipath fading channel caused by shaking the sender device. Furthermore, we implement a prototype system realizing the proposed method and evaluate the effectiveness of the proposed method. The results indicate that the proposed method can generate the same key of 128-bit length for about 3 seconds on each device.

Keywords: channel characteristics, multipass fading, near wireless communication, common key, robustness

[1] 九州大学大学院システム情報科学府
Graduate Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819–0395, Japan
[2] 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819–0395, Japan
a) tomohiro@f.ait.kyushu-u.ac.jp
b) shigeaki@f.ait.kyushu-u.ac.jp
c) arakawa@f.ait.kyushu-u.ac.jp
d) fukuda@ait.kyushu-u.ac.jp

本論文の内容は 2010 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO）シンポジウム 2010 にて報告され，ユビキタスコンピューティングシステム研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

1. はじめに

携帯電話やスマートフォンなどの小型無線端末の普及にともない，ユーザ同士が端末を持ち寄って一時的な無線ネットワーク（近距離無線ネットワーク）を形成し，互いにデータ通信を行う状況が今後ますます増えることが予想される．たとえばこのような状況として，ユーザ間での名刺や写真の交換や，会議資料の配付などが考えられる．近距離無線ネットワークの実現には，一般的に無線 LAN や Bluetooth などのデバイスが用いられるが，無線電波の届く範囲が必要以上に広いため，通信相手ではない第三者の端末まで電波が届く可能性がある．無線電波の通信範囲内にある端末には通信内容の盗聴や改ざんが容易であるので，個人情報のような重要な情報を無線によりそのまま通信するのは危険である．電波の送信電力を制限し，通信範囲を適切な範囲に調整することも考えられるが，厳密な調整は困難である．このような近距離無線ネットワークにおいて，近くにいるユーザと安全かつ簡単にデータ交換をすることが可能になれば，近距離無線ネットワークの信頼性を飛躍的に高めることになり，近距離無線ネットワークのさらなる普及につながることが予想される．

近距離無線ネットワークにおいて安全なデータ通信を実現する方法として，通信を暗号化するという手段があるが，暗号化に用いる共通鍵を第三者に知られることなく送受信端末間で共有する必要がある．公開鍵暗号を利用して共通鍵を通信相手の端末に，安全に配送する方法があるが，公開鍵暗号を安全に利用するには，通信相手の公開鍵を認証する必要がある．既存の公開鍵の認証は，インターネットへの接続が必要であり，インターネットに必ずしも接続されない近距離無線ネットワークではこのような認証が困難である．また，ユーザ同士が初対面であり互いの端末情報を知らないなどの状況も考えられる．

本論文では，近距離無線ネットワークに着目し，安全なデータ通信を実現するうえで必要な共通鍵を，送受信端末で個別に生成する手法を提案する．提案方式では，共通鍵をネットワークを介して配送せずに個別に生成することから，安全なデータ通信を実現できると考える．提案手法の主なアイデアは，送信端末を握手のように振ることにより生じる端末間の無線伝送路の変動をもとにして，同一の共有情報を各端末で個別に生成することである．端末を振ることによる伝送路の変動は，伝送路可逆性とフェージングの性質から送受信端末間でのみ受信信号強度の同一の変動として観測される．この受信電波強度の変動を各端末で符号化することにより，送受信端末間でのみ共有できる情報を生成できる．また，提案手法では，様々な種類の端末が混在し，端末の小型化が進むユビキタス社会での利用を考え，簡単かつ汎用的に共通鍵を生成できるように鍵の生成プロトコルを設計している．さらに，プロトタイプシステムを構築し，提案手法の有効性を実環境において評価した．結果から，パラメータを調整することで，約 3 秒以内に 128 bit の共通鍵を 95%以上の精度で生成することを確認した．

本論文の構成は次のとおりである．2 章では提案手法の基礎となる伝送路可逆性とフェージングについて解説し，3 章で関連研究を紹介する．4 章では端末間で同一の情報を生成する手法について説明する．5 章では提案手法の評価を行い，最後に 6 章でまとめる．

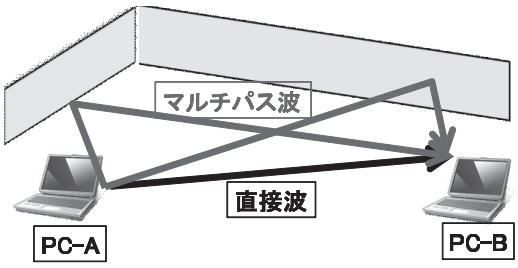
2. 伝送路可逆性とフェージング

本章では，提案手法を説明するうえで必要となる無線通信の伝送路可逆性とフェージングの概要 [1], [3], [4] を説明し，事前実験を通して，これらの性質に着目することで，端末間で同一の共通鍵を生成できることを示す．

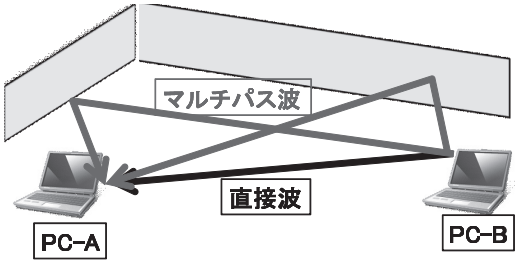
2.1 概要

図 1 (a) に示すように，無線通信デバイスを装備した 2 台の端末 PC-A と PC-B があり，PC-A から PC-B に通信した場合を考える．このような場合では，PC-A から PC-B に直接届く電波（直接波）と，電波の反射により，壁や物に衝突し複数の経路を経由して，PC-A から PC-B に届く電波（マルチパス波）が存在する．マルチパス波と直接波とは，経路長が異なるために位相が異なる波として受信端末に届き，そこで干渉を起こすことになる．この干渉が電波の強さに影響を与えることを**フェージング**という．結果として，受信端末が観測する受信信号強度（RSSI: Received Signal Strength Indication）が変動することになる．

ここで，通信に利用する電波の波長を λ，$n = \{0, 1, 2,$



(a) PC-A から PC-B



(b) PC-B から PC-A

図 1 PC-A と PC-B 間の電波の伝送路

Fig. 1 Transmission path for radio signal between PC-A and PC-B.

3,...} とすると，フェージングによる電波の強さの関係を次のように表すことができる（たとえば，λ は 2.4 GHz で約 12 cm，5 GHz で約 6 cm となる）．

$$(\text{直接波の経路長}) - (\text{マルチパスの経路長}) = n\lambda \quad (1)$$

式 (1) では，位相差がないために，直接波とマルチパス波が最も強めあう関係を示している．逆に，最も電波が弱めあう関係を式 (2) に表すことができる．

$$(\text{直接波の経路長}) - (\text{マルチパスの経路長}) = n\lambda + \frac{\lambda}{2} \quad (2)$$

式 (2) では，直接波とマルチパス波が半波長ずれるために，これらの電波は打ち消し合うことになる．実際には，直接波とマルチパス波との関係は，式 (1) や式 (2) だけでなく，様々な位相差を持つために，受信端末の受信電波が複雑に影響することになる．

次に，図 1 (a) と (b) に示すように，PC-A から PC-B への電波の伝送路と，PC-B から PC-A への伝送路を考える．PC-A から PC-B に届く際に電波がたどる伝送路は，PC-B から PC-A に届く際に電波がたどる伝送路と一致する．これを**伝送路可逆性**という．この伝送路可逆性は，直接波だけでなく，マルチパス波にもあてはまることに注意されたい．

伝送路可逆性から，直接波およびマルチパス波の PC-A から PC-B への経路と，PC-B から PC-A への経路とは等しくなることから，PC-B で観測できるフェージングの影響と，PC-A で観測できるフェージングによる影響とは等しくなる．すなわち，2 つの端末で同一の送信電力で電波を互いに送信した場合，各々の端末で観測できる受信電波の RSSI 値は等しくなるといえる．この RSSI 値は送受信端末間でしか等しくならず，第三者がこの RSSI 値を推測することは困難である．

したがって，本論文では，端末間で互いに電波を送信するような状況において，受信した電波の RSSI 値から同一の共通鍵を生成することに注目する．具体的には，端末間の電波の伝送路を意図的に変化させて，その変化にともなう RSSI の変動を各端末で個別に観測し，観測値から同一の情報共通鍵を生成することになる．

2.2 事前実験

本節では，2.1 節で説明した伝送路可逆性とフェージングの性質を利用した RSSI 値からの共通鍵の生成に関して，事前実験を通してその可能性を確認する．

実験では，無線 LAN カードを装備した 3 台の端末を用いた（**表 1**）．この 3 台の端末を**図 2** のように配置し，送信端末（以降 PC-A）を振りながら，受信端末（以降 PC-B）に向けて ping コマンドを用いてパケットを送信する．すなわち，PC-A から PC-B に ICMP Echo Request を送信し，その応答として PC-B から PC-A に ICMP Echo Reply を送信する．PC-A は PC-B が送信した Echo Reply を，PC-B は PC-A が送信した Echo Request を受信した際に，そのパケットの RSSI 値を各端末で記録する．また，盗聴端末（以降 PC-C）は PC-A が送信した Echo Request を傍受し，受信した際のパケットの RSSI 値を端末に記録する．本実験では，ping コマンドにより 1.0 ms 間隔で ICMP Echo Request を送信し，**図 3** に示すように送信端末を振る．端末を振る行為は，送受信端末間の伝送路を変化させ，フェージングの影響を変化させることを意図している．無線 LAN デバイスは IEEE802.11a を用いて，40 チャネル（5.2 GHz）を使用する．なお，ダイバーシティなどの付加設定は利用しないようにする．

結果を**図 4** に示す．図の縦軸は，パケットの RSSI 値を表し，横軸は，ICMP パケットのシーケンス番号を表す．図における菱形のプロットは，PC-B が送信し，PC-A が受信したパケットの RSSI 値（$RSSI_{Ab}$）であり，三角のプロットは PC-A が送信し，PC-B が受信したパケットの

表 1 事前実験で用いた機器
Table 1 Terminal devices used in this preliminary experiment.

	端末	型	無線 LAN カード
送信端末	Let's Note	CF-R8	IO DATA WN-WAG/CBH
受信端末	Let's Note	CF-R7	IO DATA WN-WAG/CBH
盗聴端末	Let's Note	CF-R6	IO DATA WN-WAG/CBH

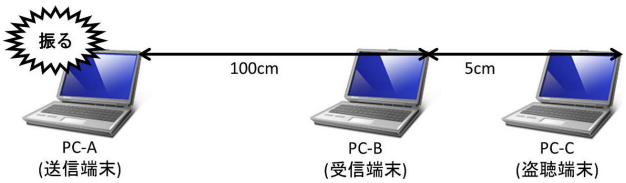


図 2 事前実験での機器の配置
Fig. 2 Location of terminal devices in this preliminary experiment.

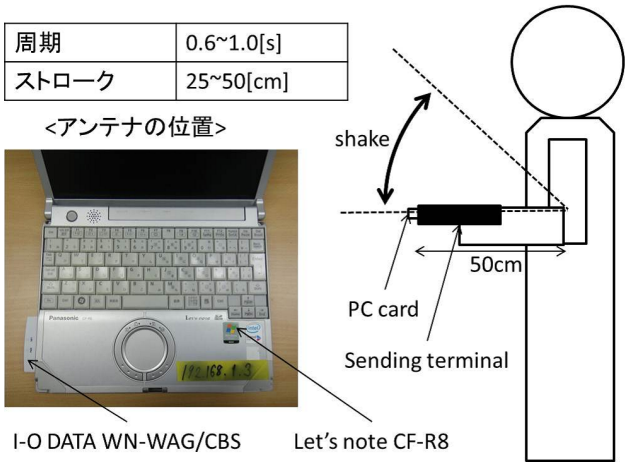


図 3 アンテナの位置と端末の振り方
Fig. 3 Method for mounting antenna and shaking terminal device.

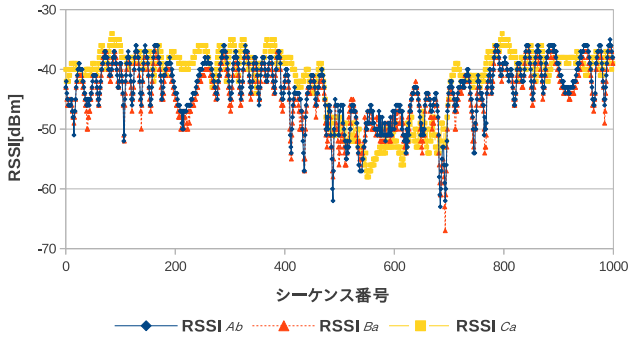


図 4 RSSI 値の変動

Fig. 4 Fluctuation of observed RSSI values in this preminary experiment.

RSSI 値（$RSSI_{Ba}$），四角のプロットは PC-A が送信し，PC-C が受信したパケットの RSSI 値（$RSSI_{Ca}$）である．

結果から RSSI 値が変動していることが分かり，また，この変動が互いの端末で相関があることが分かる．この RSSI の変動は，伝送路に依存したパラメータであり，伝送路の特性を示すものといえる．この伝送路の特性は，電波がマルチパスにより非常に複雑な伝送路を通るために，第三者には推定することが難しく，送受信端末間でのみ共有できる情報である．よって，ほぼ同時に（伝送路の変化がない程度に）電波を送受信し，RSSI 値により伝送路の特性を抽出できれば，送受信端末間でのみで共有できる共通鍵を生成できることが確認できる．ただし，両者の観測結果には雑音による若干のズレがあり，RSSI 値の変動を単純に符号化しても同一の共通鍵にならない可能性がある．また，低い周波数の RSSI の変化は，振ることにより端末間の距離が変動することで生じるものであり，盗聴者は推定・観測することができる．提案手法では，RSSI 値の変動から頑健に同一の共通鍵を生成するとともに，盗聴者が推定できる変動と雑音によるズレを排除することにより正規の通信者間のみが共通鍵を生成する手法を実現する．

3. 関連研究

本章では伝送路可逆性を利用して，共通鍵を生成する方式の関連研究について紹介する．伝送路可逆性を用いて通信者間で共通鍵を生成するためには，電波伝送路を変動させることと伝送路特性を抽出することが必要である．伝送路に変化を与える手法として，民生品向け可変指向性アンテナとして開発中のエスパアンテナを用いて電波伝送路を変動させる手法 [1] や，複数アンテナを切り替えることで変動させる手法 [2] などがある．また伝送路特性を抽出する手法として，遅延プロファイルを用いた手法 [3] や OFDM（Orthogonal Frequency Division Multipplex：直交周波数領域多重方式）などプロトコルを利用した手法 [4] などがある．各手法の詳細を下記に述べる．

文献 [1] において，エスパ（ESPAR: Electronically Steerable Prastic Array Radiator）アンテナを用いた IEEE802.15.4 無線秘密鍵共有システムが提案されている．民生品向け可変指向性アンテナとして開発中のエスパアンテナを用いて，電波伝送路を大きく変動させることにより，電波伝送路の時間変動の少ない環境においても，秘密鍵を高速に生成することを可能にしている．具体的には，エスパアンテナのビームパターンをランダムに変化させながら正規の通信者間で RSSI 値を測定し，得られた RSSI 値を 2 値化することで共通鍵を生成している．128 ビットの共通鍵を 3 秒周期で生成するシステムの鍵生成成功確率が 99.998%以上となることが実験により示されている．

文献 [2] においてアンテナ切替えと RSSI 値の比較によって電波伝送路の時間変動が小さい環境でもランダムな共有情報を生成する方式が提案されている．複数アンテナ構成を持つ端末を用いて，TDD（Time Division Duplex：時分割復信方式）により高速に送受信を行い，各アンテナで受信した信号の大小比較をそれぞれの端末で行い，2 値化することで共通鍵を生成している．各端末で送受信用のアンテナを 2 本ずつ用いた場合と，3 本ずつ用いた場合に対して計算機シミュレーションを実施し，結果として 3 本ずつ用いた場合において十分な特性を得られることが示されている．

文献 [3] において，UWB（Ultra Wide-Band）における遅延プロファイルに基づく秘密共有方式が提案されている．この研究では，直接波とマルチパス波との間の到達時間差を 2 つの正規局間で測定することにより共通鍵を生成している．性能を評価するために無線 PAN 環境を想定し計算機シミュレーションを実施している．結果，SN 比が 25 dB の場合に秘密鍵共有がほぼ可能であることが確認されている．

文献 [4] において，陸上通信における OFDM の伝送路特性に基づく秘密鍵共有方式が提案されている．OFDM に適した時変周波数特性に基づいて，共通鍵を生成している．伝送路の可逆性に基づき時変周波数特性を交互に測定し，鍵生成誤り対策として伝送路特性の測定時間差補償，同期加算処理による雑音軽減，代数的復号法による鍵不一致訂正などを適用している．また鍵の安全性を独立性評価法により検討している．OFDM を利用した IEEE802.11a の無線 LAN に準拠したモデルを構成し，計算機シミュレーションを実施した結果，SN 比 15 dB の現実的な設定において，秘密鍵共有が可能であることが確認されている．

上に記述した手法は特別なデバイスなどを用いるために精度も良く，生成するために必要な時間も小さい．一方でスマートフォン，タブレット端末やノート PC の普及により特別なデバイスを用いずに，標準搭載された通信デバイスのみで共通鍵を生成する手法が注目されている [5]．具体的には，端末を持った人が歩くことにより伝送路に変化を与え，電波伝送路の特性をフェージングにより変

動したRSSI値から抽出する手法である．文献 [6] において，様々な環境において1秒間に20回Beaconを送受信し合った際のRSSIに対して，文献 [1] および文献 [7], [8], [9] で提案された手法に加えて，ASBG（Adaptive Secret Bit Generation）を適用させ，生成できる共通鍵の長さや品質について検証している．検証結果から，端末を持って歩くなど，電波伝送路が動的に変化する環境において，1秒間に数ビット程度の共通鍵を生成できることを示している．ただし，図4で見られるような，盗聴者が正規の通信者の非常に近く（使用電波の波長の数倍以内）に存在した場合において，盗聴端末が測定したRSSI値と，正規の送受信者間が測定したRSSI値との間に，ある程度の相関が存在することが示されている．

本研究も特別なデバイスなどを用いずにRSSIのフェージング結果から共通鍵を生成することを目的としている．ただし，伝送路を変動させる手法として，人が歩くことにより端末を移動させるのではなく，握手のように端末を振る手法に着目している．文献 [10], [11] で，加速度センサを搭載した端末を振ることで共通鍵を生成する方式が提案されている．本研究が対象とする近距離無線通信を確立するために人がとる行動として，端末を移動させるより握手のように端末を振るほうが親和性が高い．また，歩くことよりも端末を振ることの方が，電波伝送路をより変化させることができ，結果として，共通鍵を生成する速度を高めることができる．さらに端末を振ることにより，伝送路特性のみを抽出しやすくなり，盗聴者が盗聴しにくい共通鍵を生成できる．このように，特別なデバイスを用いなくても，端末を振ることに注目することで，従来より盗聴されにくく，高速に共通鍵を生成できると考える．

4. 提案手法

本章では，2.2節で示したRSSI値の変動に相関があることを利用し，通信路の暗号化に利用できる共通鍵を配送することなく送受信端末間で生成する手法を提案する．本手法の設計方針として以下のことをあげる．

- 特別なデバイスやプロトコルの指定をしない．受信時のRSSI値を測定できればよい．本論文では，ICMPのEcho RequestとReplyを利用しているが特に指定しない．
- ユーザの利用負荷が小さい．すなわち，短い時間で大きな共通鍵を誤り少なく共有する．

電波伝送路を変動させる手法として端末を振る手法をとり，伝送路特性を抽出する手法として標準搭載されている機器で測定できるRSSI値を用いる．ただし，RSSI値は雑音も多く，短い時間に大きな共通鍵を生成することは難しい．さらに，盗聴端末が正規の通信者端末の非常に近くに存在する場合に，正規の通信端末間で得られたRSSI値と，盗聴端末が傍受したRSSI値とに相関がある問題がある．そこでRSSI値の変動を周波数領域上で解析し，盗聴が困難なフェージングによる変動のみを抽出する．これにより，雑音成分を極力排除し，盗聴者に推定されにくい部分のみで送受信端末間で安定して共通鍵を生成することを目指す．

提案方式は，共通鍵を生成するために，“RSSI履歴の作成”，“フィルタリング”，“除去”，“符号化”の4つのフェーズから構成される．以下，この4つのフェーズについて詳しく説明する．

4.1 RSSI履歴の作成

本論文では，RSSIの時間遷移を記録したものRSSI履歴と呼ぶことにする．まず，送受信端末間でICMPパケットを送受信することでRSSI履歴を作成する手順について説明する．

［RSSI履歴作成手順］

ステップ1：ユーザは伝送路に変化を与えるために端末を振る．

ステップ2：送信端末が受信端末にEcho Requestを設定したパケット数だけ送信する．

ステップ3：Echo Request到着後，受信端末が送信端末にEcho Replyを送信する．

ステップ4：受信端末が送信端末から送られてきた各Requestの RSSI値と，そのシーケンス番号を関連づけを行い，RSSI履歴を作成する．

ステップ5：送信端末が受信端末から送られてきた各Replyの RSSI値と，そのシーケンス番号を関連づけを行い，RSSI履歴を作成する．

上記のような手順で，送受信端末上でRSSI履歴を作成し，そのRSSI履歴から共通鍵を生成することになる．送受信端末で測定したRSSI履歴が，伝送路可逆性の原理から高い相関にあるためには，送信端末がEcho Requestを送信してから，受信端末からのEcho Replyを受信するまでの間（応答時間）に，伝送路の変化が少ない必要がある．上記の手順では応答時間内に，振ることにより端末が移動するので，送受信における伝送路は完全には一致しない．しかし，応答時間が短い場合では，この伝送路の変化は，ほとんど影響しないと考えられる．たとえば，2.2節の事前実験における応答時間は，平均0.1 msであった．仮に端末を振る速さが5 m/sだとしても，0.1 msの間に端末が移動する距離は，約0.5 mmである．事前実験で使用した電波の波長が，数センチ（5 GHz帯で約6 cm，2.4 GHz帯で約12.5 cm）であり，フェージングの影響（強め合う，弱め合う）が半波長で反転することを考慮すると，伝送路の変化はほとんど影響しないと考えられる．もし，何らかの影響で応答時間が増大した場合，RSSI履歴上で急激な変動としてその影響が現れるが，提案手法では急激な変動付近の除去法を用いて，このような場合に対処している．詳細

は 4.3.2 項において述べる．

4.2 フィルタリング

本節では，4.1 節で作成した RSSI 履歴から，電波伝送路の変化による変動だけを抽出するためにフィルタリング手法を提案する．具体的には RSSI 履歴の変動を周波数領域上で解析し，雑音部分の影響や盗聴者から盗聴されやすい低周波数の変動をを極力除去し，端末を振ることにより変動したフェージング結果のみを抽出する．RSSI 履歴の変動を周波数領域上で解析すると，変動の要因を以下のように考えることができる．

要因 1：小型端末を振ることにより，送受信端末間の距離が変動し，RSSI 値が変動する．

要因 2：小型端末を振ることにより，直接波およびマルチパス波の伝送路に変化が生じ，フェージングの影響が変化することから，RSSI 値が変動する．

要因 3：雑音により，RSSI 値が変動する．

これらの要因を周波数領域上でモデル化したものを**図 5** に示す．要因 3 は白色雑音と考え，すべての周波数に影響を与える．また，白色雑音が RSSI 値に与える影響の度合いは，要因 1 や要因 2 に比べて小さく，また送受信端末間で相関がないことが特徴的である．

要因 1 の変動の周期は，人間が手で小型端末を振る周期とほぼ一致すると考えられる．また，人間が小型端末を振る速さには限界があることから，その変動は非常に低い周波数部分に影響を与えると考えられる．要因 1 が RSSI 値に与える影響の度合いは大きく，かつ送受信端末間でそれらの間に相関があると予想できる．しかし，手の振りを見ている第三者が予測可能である．

要因 2 においても RSSI 値に与える影響の度合いは，2.2 節で述べたように送受信端末間で相関があると考えられる．要因 1 とは異なり第三者が推測することは困難である．また，その度合いは，マルチパス波が非常に複雑な経路を通るために，様々な周波数に影響を与えると考えられる．特に，低い周波数成分ほど，その影響が大きいと予想される．逆に，高い周波数成分では，白色雑音に打ち消されてしまうため影響をほとんど与えない．したがって，要因 1 が影響を及ぼす範囲よりも大きく，雑音に打ち消されない範囲の周波数成分を抽出すれば，要因 2 の影響を最大限に抽出できると考えられる．5.2 節において，以上の議論の正当性を実験により示す．

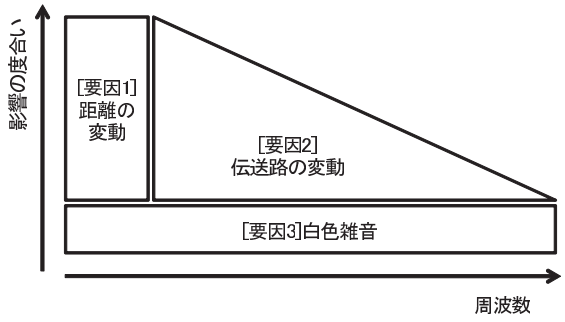


図 5 RSSI 値の変動の周波数領域上でのモデル
Fig. 5 Modeling fluctuation of RSSI values in frequency domain.

提案手法では，有効な RSSI 履歴の周波数成分を抽出するために，α Hz〜β Hz のバンドパスフィルタにかけることにしている．ここで，α，β は，チューニングパラメータである．以降，RSSI 履歴におけるシーケンス番号 seq の RSSI 値を RSSI(seq) で表す．また，RSSI 履歴を周波数上に分解し，α Hz〜β Hz を利用して復元した後，時間軸上（すなわちシーケンス番号上）に復元した結果を $FilteredRSSI(seq)$ で記述し，β Hz 以上を利用して復元した結果を $NoiseRSSI(seq)$ と記述する．

4.3 除去

本節では *FilteredRSSI* 履歴から共通鍵を生成する際に，端末間で異なる共通鍵を生成する確率が高い箇所を除去し，符号化の際に誤りが発生する確率を抑える手法を提案する．端末間で異なる共通鍵を生成する確率が高い箇所として以下がある．

箇所 1：符号化の際に利用する閾値の付近．

箇所 2：*FilteredRSSI* 履歴における急激な変動の付近

基本的な符号化の方法は，0 を閾値として，閾値との大小関係で 2 値化することになる．この方法を観測した各シーケンス番号ごとに適用することで，最終的なビット列を生成する．しかし，箇所 1 のように閾値付近の値でかなりの可能性で誤りが発生してしまう．たとえば，送信端末で RSSI 値として 0.1 を観測し，受信端末で −0.1 を観測した場合では，これらの値は非常に近いのだが異なる値に符号化されることになる．このために，提案手法では，文献 [1] の手法を基にした閾値付近の除去法を提案し適用する．

また，変動が緩やかな箇所（すなわちピーク時）は誤りが少なく，箇所 2 のように変動が急激な箇所では誤りが多い傾向がある．このため，提案手法では，閾値付近の除去法に加え，急激な変動付近の除去法を新たに考案し適用することで，符号化の際に誤りが発生する確率をさらに小さくする．

4.3.1 閾値付近の除去法

最初に，閾値付近の除去法の詳細について説明する [1]．上述したように，**図 6** のように，閾値よりも大きければ 1，小さければ 0 と符号化した場合，閾値付近で誤りが生じる．このため，どちらか一方の端末で観測した RSSI 値が閾値付近である場合，誤りが高確率で発生すると考えてその箇所は情報生成に利用しない．本提案手法では，雑音が多く含まれると RSSI 値のずれが大きくなることに注目し，文献 [1] の閾値付近の除去法をさらに発展させ，閾値付近の除去の割合を各端末で観測される雑音の大きさによ

り動的に変化させる手法を提案する．本提案手法では，雑音は白色雑音であると仮定し，4.2 節の *NoiseRSSI* 履歴の標準偏差を閾値付近の除去に用いる．閾値付近の除去に関する手順を下記に示す．

［閾値付近の除去手順］

ステップ 1：各端末で観測した RSSI 履歴を周波数分解する．

ステップ 2：各端末で *FilteredRSSI* 履歴と *NoiseRSSI* 履歴を計算する．

ステップ 3：各端末で *NoiseRSSI* 履歴の標準偏差 Std_{Noise} を計算する．

ステップ 4：各端末で以下の条件を満たすシーケンス番号群を抽出する．

$$|FilteredRSSI(Seq)| < c \times Std_{Noise}$$

ただし，c は閾値付近の除去の割合を決定する閾値付近の除去係数とする．

ステップ 5：抽出されたシーケンス番号群を端末間で交換する．

ステップ 6：どちらか一方の端末において抽出されたシーケンス番号を破棄する．

手順を経て，図 6 に閾値付近の除去法を適用した結果を**図 7** に示す．実線は PC-B が送信し，PC-A が受信したパケットの RSSI 値にフィルタリングした値（$FilteredRSSI_{Ab}$ 履歴）であり，また点線は $FilteredRSSI_{Ba}$ 履歴である．図 7 の四角のプロットは $FilterdRSSI_{Ab}$ 履歴に，菱形のプロットは $FilterdRSSI_{Ba}$ 履歴に閾値付近の除去法を適用した後に残ったシーケンス番号に対応した値を示している．

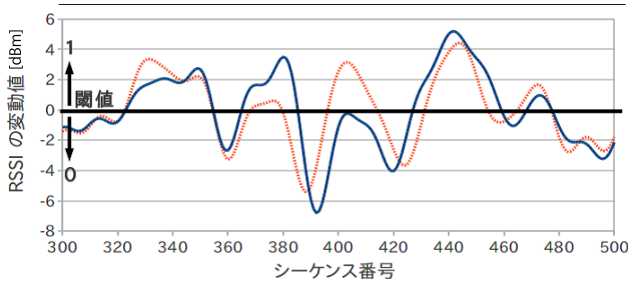


図 6 閾値付近の除去法適用前

Fig. 6 Fluctuation of observed RSSI values before the elimination.

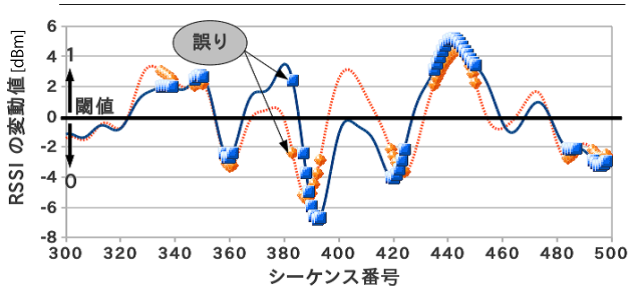


図 7 閾値付近の除去法適用後

Fig. 7 Fluctuation of observed RSSI values after the elimination.

4.3.2 急激な変動付近の除去法

次に，急激な変動付近の除去法の詳細について説明する．上述したように，*FilteredRSSI* 履歴に大きな変動があったときに誤りが発生しやすい．たとえば図 7 のシーケンス番号 385 番の周辺では変動が急であり，誤りが発生していることが分かる．そこで，どちらか一方の端末で生成した *FilteredRSSI* 履歴の変動が大きい場合，誤りが高確率で発生すると考えて，その箇所は共通鍵生成に利用しない．変動が大きいと判断するために，$DevFilteredRSSI(Seq) = FilteredRSSI(Seq+1) - FilteredRSSI(Seq)$ と定義した *DevFilteredRSSI* 履歴の標準偏差を用いる．急激な変動付近の除去に関する手順を下記に示す．

［急激な変動付近の除去手順］

ステップ 1：各端末で *FilteredRSSI* 履歴を計算する．

ステップ 2：各端末で *FilteredRSSI* 履歴から *DevFilteredRSSI* 履歴を計算し，その標準偏差 Std_{Dev} を計算する．

ステップ 3：各端末で以下の条件を満たすシーケンス番号群を抽出する．

$$|DevFilteredRSSI(Seq)| > k \times Std_{Dev}$$

ただし，k は急激な変動付近の除去の割合を決定する変動による除去係数とする．

ステップ 4：抽出されたシーケンス番号群を端末間で交換する．

ステップ 5：少なくともどちらか一方の端末において抽出されたシーケンス番号を破棄する．

上記の手順を経て，図 7 に急激な変動付近の除去法を適用した結果を**図 8** に示す．図 8 の四角のプロットは $FilteredRSSI_{Ab}$ に，菱形のプロットは $FilteredRSSI_{Ba}$ に閾値付近の除去法と急激な変動付近の除去法を適用した後に残ったシーケンス番号に対応した値である．

閾値付近の除去法や急激な変動付近の除去法の各ステップ 4 において，除去するシーケンス番号を通信を使って相

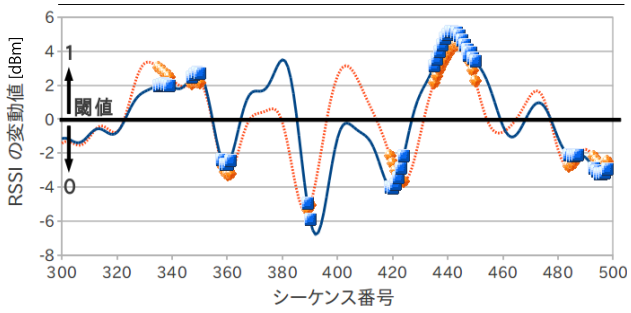


図 8 閾値付近の除去法，および急激な変動付近の除去法適用後

Fig. 8 Result after eliminating RSSI values around the threshold and sharp fluctuation.

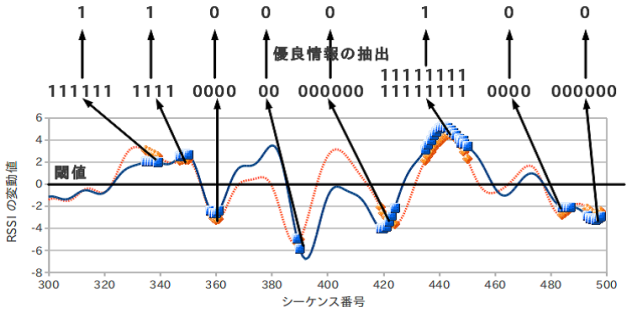


図 9 優良情報の抽出の例

Fig. 9 An example of extracting high quality keys.

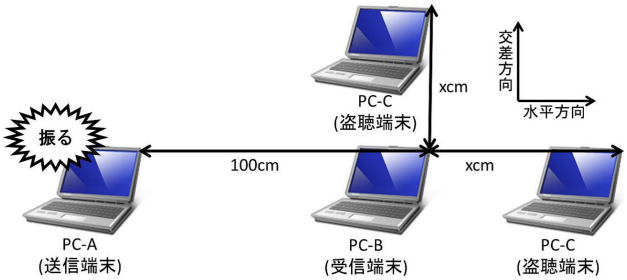


図 10 実験の様子

Fig. 10 Location of terminal devices in this experiment.

手に伝える過程がある．この伝達はすべてのシーケンス番号について符号化を終了した後，一括して行うことになる．しかし，除去した情報が，第三者に傍受される可能性がある．そのために，共通鍵の符号化は，除去された箇所から推測できないように符号化する必要がある．

4.3.3 優良情報の抽出

本項では，上記で述べた除去箇所から共通鍵の推測を防ぐために，文献 [5] でも紹介されている符号化したビット列から優良情報のみを抽出する手法を利用する．閾値付近の除去法，および急激な変動付近の除去法により除去されたシーケンス番号を第三者は盗聴可能である．これにより，第三者は閾値付近であった箇所や変動があった箇所が分かり，さらにパケットの送信間隔が短い場合では，閾値をまたいでいない部分も分かる．すなわち，生成した情報の中で特定のビットが連続する部分も分かることになる．このため，提案手法では，**図 9** のように，同一のビットが連続して続く部分をまとめるようにする．すなわち，「1111」や「000」を「1」や「0」にまとめることで，共通鍵の品質を向上させる．

5. 評価

本章では，実環境における提案手法の評価を行う．具体的には，特別なデバイスを用いずに，盗聴しにくい共通鍵を高速に生成できるかについて検証する．最初に，評価に必要となるデータセットの作成手順，および作成環境について述べる．次に，4.2 節で述べたバンドパスフィルタの有用性について，相関係数からみれる本手法の堅牢性という観点から検証する．最後に必要とする共通鍵の長さを得るのに必要な時間と，そのときに誤りなく生成できる確率について，閾値付近の除去法と急激な変動付近の除去法の除去幅との関係について検証を行う．

5.1 データセット

文献 [6] では，電波伝送路の特性を RSSI 値を用いて抽出する方式について，以下のような盗聴者モデルを想定し，その手法の堅牢性を示している．

(1) 盗聴者は，正規の通信者の通信をすべて傍受可能とする．

(2) 盗聴者は，共通鍵生成のアルゴリズム，および，その設定値をすべて把握しているとする．

(3) 盗聴者は，正規の通信者に非常に近い場所（使用電波の波長の数倍以下）以外であれば，自由に移動し傍受可能とする．

(4) 盗聴者は，受動的な盗聴者であり，ジャム信号を送信して通信を妨害したり，なりすまし攻撃，中間者攻撃といった攻撃的な盗聴は行ったりしないものとする．

ただし，上記の (3) で，正規の通信者に非常に近い場所については検証の対象から除外されている．また，これらの場所は，文献 [14] や [15] において，盗聴者の測定値と正規の受信者の測定値との間に，高い相関が存在することが示唆されている．これから，送受信者の周辺，および送信者と受信者を結ぶ直線上について，データセットを生成し評価すれば，本手法の有効性を示すことができると考える．

本評価で使用するデータセットを次のようにして作成する．縦 6 m，横 12 m の部屋の中央で，送信端末（PC-A），受信端末（PC-B），盗聴端末（PC-C）を**図 10** のように配置する．盗聴端末を，送信端末と受信端末を結ぶ直線の交差方向に，受信端末から 1 cm から 100 cm の範囲で離れた箇所に配置し，それぞれの箇所で 4.1 節で述べた事前実験と同じ方法で 10 回ずつ測定する（測定 1）．水平方向も同様に測定する（測定 2）．すなわち，測定 1 と測定 2 で盗聴端末を 60 カ所に配置し，合計 600 回の測定を行う．上記の測定以外に，盗聴端末を静止させて盗聴するだけでなく，盗聴端末を送信端末と同様に振りながら盗聴する場合についても測定したが，結果として，静止した場合とほぼ同等か逆に精度が下がったために，今回は静止した場合のみ結果を紹介する．

5.2 RSSI 変動の周波数分析

本節では，4.2 節で述べたバンドパスフィルタのバンド幅を決定するための調査と，相関係数からみれる本手法の堅牢性について検証する．最初に，測定した RSSI 履歴の相関を**図 11** に示す．今回，RSSI の相関を表す指標として，相関係数を用いた．PC-B が送信し，PC-A が受信したパケットの RSSI 値の履歴（$RSSI_{Ab}$ 履歴）と，PC-A が送信

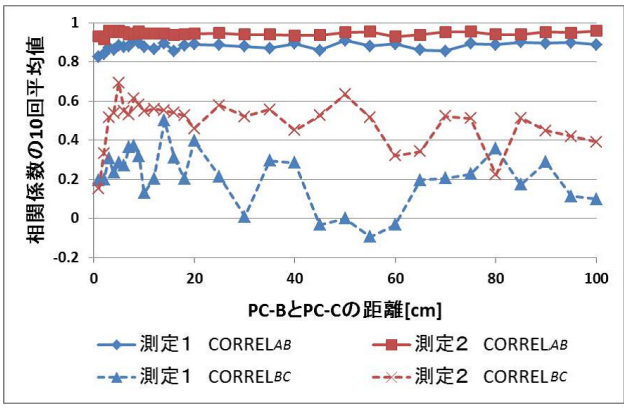


図 11 バンドパスフィルタ適用前の相関係数と盗聴者の位置の関係
Fig. 11 Relation between correlation coefficient and distance before using bandpass-filter.

し，PC-B が受信したパケットの RSSI 値の履歴（$RSSI_{Ba}$ 履歴）の相関係数を $CORREL_{AB}$ とする．同様に，$RSSI_{Ba}$ 履歴と，PC-A が送信し，PC-C が受信したパケットの RSSI 値の履歴（$RSSI_{Ca}$ 履歴）の相関係数を $CORREL_{BC}$ とする．図 11 から，送受信者の周辺，および送信者と受信者を結ぶ直線上において，盗聴者の測定値と正規の送受信者の測定値の相関が高くなる箇所があることが分かる．具体的には，測定 2 の x = 5 の場合において，正規の送受信者間の相関が 0.96 に対して，盗聴者の相関が 0.69 と最も高い値を示した．

次に盗聴者との相関を下げるためにパラメータ α，β を決定する．データセットの中で，盗聴者の測定値と正規の送受信者の測定値の相関が最も高かった，測定 2 の x = 5 cm のデータについて分析を行う．**図 12** は，$RSSI_{Ab}$ 履歴，$RSSI_{Ba}$ 履歴のそれぞれを 500 Hz まで周波数分解し，α〜β Hz でフィルタリングした後の $FilteredRSSI_{Ab}$ 履歴と $FilteredRSSI_{Ba}$ 履歴の相関関係を調べた結果である．また，**図 13** は $RSSI_{Ca}$ 履歴を 500 Hz まで周波数分解し，α〜β Hz でフィルタリングした後の $FilteredRSSI_{Ca}$ 履歴と $FilteredRSSI_{Ba}$ 履歴の相関関係を調べた結果である．図 12 から分かるように，α が 5 以下の場合，正規の通信者間で高い相関が得られる．しかしながら，図 13 から，これらの場合においては，盗聴者との相関も高くなることが分かる．これは，直接波による変動を考慮しているためだと考えられる．また，β を小さく設定すると，α の値によらず，盗聴者との相関が高くなることが分かる．これらのことから，α と β を小さくしすぎずに，β と α の差が極力大きくなる値を設定すればよいことが分かる．本実験では，$\alpha = 20$ および $\beta = 80$ のときに，正規の通信者間の相関と，盗聴者との相関の差が最も大きくなることが分かった．

今回用意したすべてのデータセットに対して，$\alpha = 20$ および $\beta = 80$ のバンドパスフィルタを適用させた結果を**図 14** に示す．なお，$FilteredRSSI_{Ab}$ 履歴と $FilteredRSSI_{Ba}$ 履歴の相関係数を $FilteredCORREL_{AB}$，$FilteredRSSI_{Ca}$ 履歴

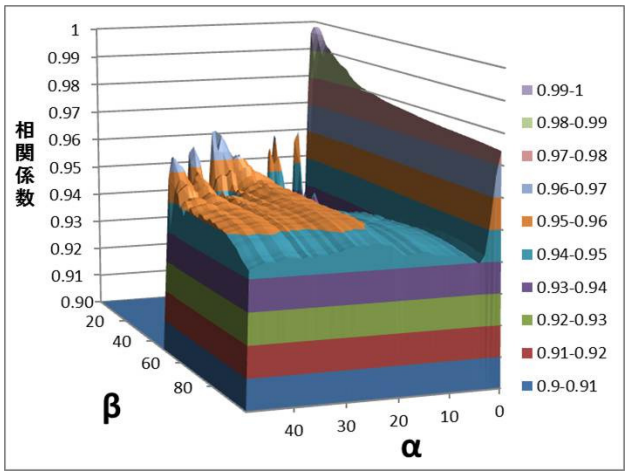


図 12 バンドパスフィルタが正規の送受信者間の相関に与える影響
Fig. 12 Effect of bandpass-filter on correlation between PC-A and PC-B.

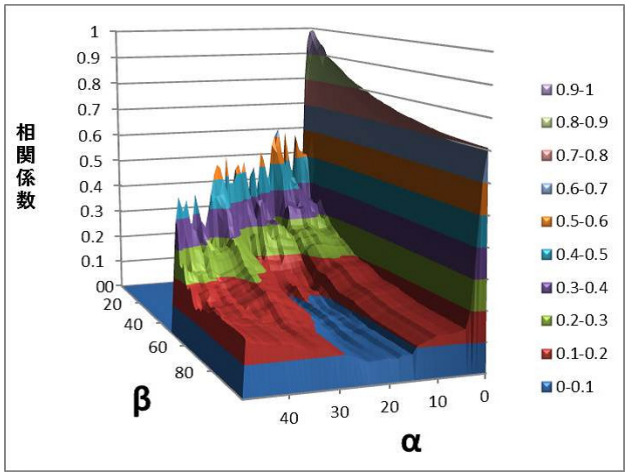


図 13 バンドパスフィルタが盗聴者と受信者との相関に与える影響
Fig. 13 Effect of bandpass-filter on correlation between PC-B and PC-C.

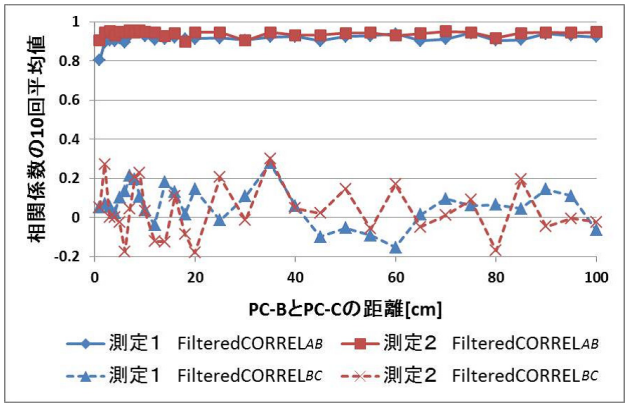


図 14 バンドパスフィルタ適用後の相関係数と盗聴者の位置の関係
Fig. 14 Relation between correlation coefficient and distance after using bandpass-filter.

と $FilteredRSSI_{Ba}$ 履歴の相関係数を $FilteredCORREL_{BC}$ とする．また，測定 1，測定 2 それぞれすべてのデータセットに適用した結果の相関係数の平均値（300 回平均）を**表 2**

表 2 バンドパスフィルタ適用前後での相関係数の平均
Table 2 Terminal devices used in this preliminary experiment.

	相関係数	提案手法適用前	提案手法適用後
測定 1	正規の通信者間	0.88	0.92
	盗聴者と受信者	0.21	0.06
測定 2	正規の通信者間	0.95	0.94
	盗聴者と受信者	0.49	0.03

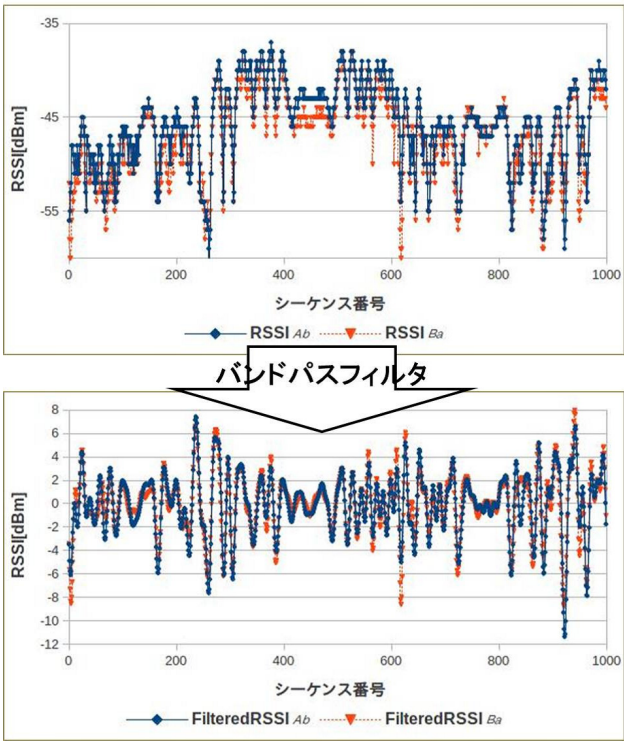


図 15 $\alpha = 20$, $\beta = 80$ の際の RSSI 履歴と FilteredRSSI 履歴の比較
Fig. 15 Fluctuation of RSSI values after using bandpass filter.

に示す．表から，$\alpha = 20$ および $\beta = 80$ のバンドパスフィルタにより，正規の送受信者の相関を低下させることなく，盗聴者との相関のみを低くすることができていることが分かる．特に，測定 1 および測定 2 ともに，盗聴者との相関の著しい低下を確認できる．またバントパスフィルタ適用後の具体的な RSSI 履歴を**図 15** に示す．図からも適用後の波形の一致度が適用前と比べて向上していることが分かる．以上の結果から，ある特定のバンドパスフィルタ，今回の場合は 20〜80 Hz のバンドパスフィルタを適用すれば，盗聴が困難なマルチパス変動を抽出できることを確認できる．

5.3 共通鍵の生成実験

本節では，実際に共通鍵を生成し，生成した共通鍵を評価する．本評価では，128 ビットの共通鍵を生成することを目標としている．これは，米国の新暗号規格である AES（Advanced Encryption Standard）[16] での利用を想定しているためである．AES では，鍵長として 128 ビット，

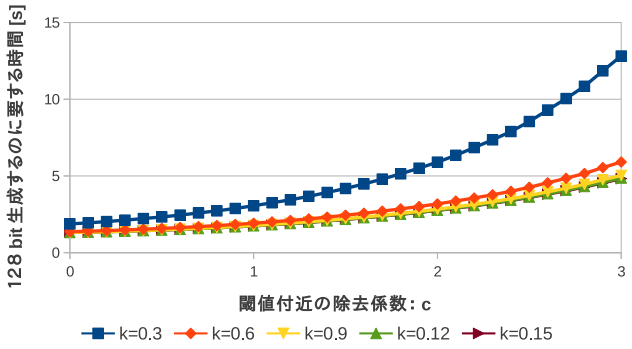


図 16 128 ビット生成するのに必要な時間
Fig. 16 Time required for generating 128 bits secret key.

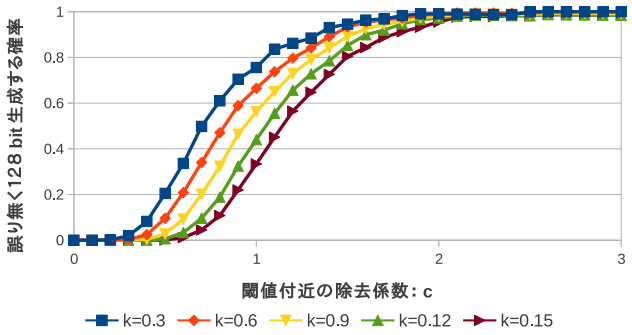


図 17 誤りなく 128 ビット生成することができる確率
Fig. 17 Probability for generating 128 bits secret key without any miss.

192 ビット，256 ビットの中から選択できるが，本論文でターゲットとする近距離無線ネットワークが一時的なネットワークであり，同一の共通鍵を永続的に利用しない（使い捨てである）点，および携帯端末での利用を想定しているため計算負荷を極力抑えることが必要な点を考慮するため，128 ビットを目標値とした．

次に 4.3 節で提案した手法を用いて，共通鍵を生成する．まず最初に，$\alpha = 20$ および $\beta = 80$ においてバンドパスフィルタを適用した結果に対して，提案手法のパラメータである除去係数 c を 0.0〜1.0 の範囲で，除去係数 k を 0.0〜1.5 の範囲でそれぞれ変化させ，各パラメータの値を用いて符号化した結果について分析する．今回は 128 ビットの共通鍵を得るのに必要な時間（**図 16**）と，そのときに誤りなく生成できる確率（**図 17**）について分析する．

図 16 と図 17 の比較から分かるように，必要とする共通鍵の長さを得るのに必要な時間と，そのときに誤りなく生成できる確率はトレード・オフの関係にある．そのため，利用シーンに応じて c と k を適切に調整する必要がある．例として，$c = 1.8$, $k = 0.9$ のときについて考える．このときの 128 ビット生成するのに必要な時間は 2.56 秒であり，誤りなく 128 ビットを生成することができる確率は 0.958 であった．これは，本提案方式と同様に RSSI を用いて共通鍵を生成する文献 [6] の方式が，1 秒間に数ビットしか生成できないことを考えると，非常に高速に共通鍵を生成で

表 3 生成情報の品質評価
Table 3 Evaluation of secret keys.

評価項目	$c = 1.8$ $k = 0.9$	$c = 3.0$ $k = 0.3$	$c = 0.9$ $k = 1.5$
128 ビット生成するのに必要な時間 [s]	2.56	12.81	1.68
誤りなく 128 ビット生成することができる確率	0.96	1.00	0.22
$Prob(0,0)$	0.087	0.158	0.065
$Prob(1,0)$	0.402	0.297	0.428
$Prob(0,1)$	0.402	0.296	0.429
$Prob(1,1)$	0.109	0.249	0.078

きるといえる．

最後に，生成した共通鍵の品質について考察する．図 15 で使用したデータに対して，$c = 1.8$，$k = 0.9$ で符号化した結果，次のような共通鍵を得ることができた．

01100101001010101100101010010101010100101011011

このような共通鍵を，600 試行で，約 3 万ビット生成することができた．この共通鍵についての品質を『00』『01』『10』『11』の発生確率を用いて評価する．生成した共通鍵において，『1』が生成される確率を $Prob(1)$ とし，『1』のあとに『1』が生成される確率を $Prob(1,1)$ として，$Prob(0,0)$，$Prob(1,0)$，$Prob(0,1)$，$Prob(1,1)$ の値を**表 3** に示す．表から，生成された共通鍵には偏りがあるが，c と k によりその偏りの大きさが変動することが分かる．具体的には，$c = 3.0$，$k = 0.3$ のときは，$c = 0.9$，$k = 1.5$ や，$c = 1.8$，$k = 0.9$ のときに比べ，鍵の偏りは緩和されている．このことから，鍵の品質を向上させるためには，c と k を適切に設定する必要がある．

また，生成した共通鍵を通信路の暗号化などで利用する場合，送受信端末間で共通鍵が 1 ビットでも異なると利用できない．このことは長いビットの共通鍵を生成する場合の課題となる．この課題に対して，たとえば，共通鍵の生成後に，その情報の誤り訂正符号を交換し訂正することで，誤りビット数をある程度許容できると考える [12], [13]．また，共通鍵のハッシュ値を交換し，共通鍵が互いに一致しないことだけを確認できるようにし，一致しなければ情報を再度生成するようなアプローチもとることができる．このようなアプローチと組み合わせて，必要なビット長と誤りビット数とを統合的に考えて，α，β，c，k の値をうまく調整する必要がある．

5.4 考察

本評価では，実験環境として，屋内の部屋（6 m × 12 m）で行い，送信端末と受信端末の位置関係は一定とし，一定の振り方で測定を行った．また，利用チャネル，パケット送信間隔も一定の値とし，送受信端末は同じ端末と同じ PC カードを利用した．これらは，鍵生成の性能に大きく影響を与える可能性がある．これらのパラメータが本手法に与える影響について以下に考察する．

環境：文献 [14] では，マルチパスが発生しにくい環境の方が盗聴が容易であることが述べられている．この理由は，盗聴を困難にする要因が，複雑に反射するマルチパスであり，マルチパスが発生しにくい環境では，推測が容易な直接波の変動のみで共通鍵を生成するためである．提案手法はマルチパスに基づき共通鍵を生成することに着目しているため，評価はある程度マルチパスが発生する環境（6 m × 12 m の屋内の部屋）で評価を行った．しかしながら，マルチパスが発生しにくい環境における提案手法の性能評価は，提案手法の実用化に向けて重要な課題である．

端末の状態：提案手法は携帯端末での利用も想定している．そのため，送信者と受信者が移動するシーン（歩行など）についても考察すべきである．2.2 節で示したように，送受信者間の ping の応答時間が短いために，応答時間内に端末が移動する距離は，性能に大きな影響を与えないと考えられる．具体的には，一般的な歩行速度を 4 km/h とすると，2.2 節で示した端末の移動速度が秒速 5 m/s（時速に換算すると時速 18 km/h）の場合と比べて，応答時間内に端末が移動する距離は短く，移動による影響は少ないと考えられる．また，送信者を歩かせた実験を実際に実施しており，静止している場合とほぼ変わらない結果が得られている．

デバイス誤差：RSSI の計測方法はベンダ依存のものであり，デバイスが異なるとその測定値は異なることが考えられる．本手法では絶対値でなく，相対値を使用するので，絶対値を利用するよりもデバイス固有の誤差を吸収できると考えている．このことを検証するために，異なる PC カード（送信端末：IO DATA WN-WAG/CBH，受信端末：NEC AtermWL54SC2）を用いて，4.1 節で述べた事前実験と同じ要領で 10 回測定を行った．10 回の測定結果から，送受信者間の相関は平均 0.90 であり，同一の PC カードを用いた場合とほぼ同じであった．しかし，今回用いた，PC カードは形状は違うものの，どちらも同じ Atheros の無線 LAN チップを搭載している．無線 LAN チップが異なり RSSI の測定方法が大きく異なる場合は，今回の実

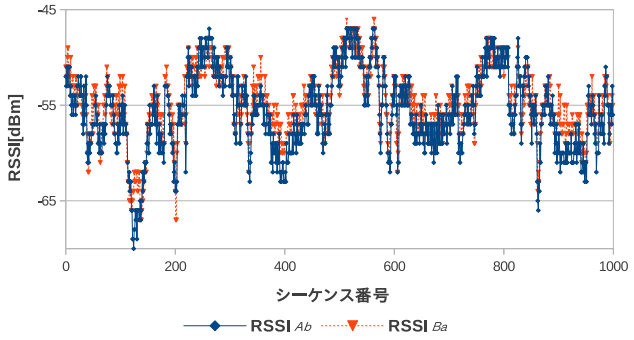


図 18 2.4 GHz における実験
Fig. 18 Fluctuation of RSSI values useing 2.4 GHz.

験ほど精度は良くないと考えられる．文献 [6] では，Atheros と Intel の無線 LAN チップを混在させた場合において，RSSI 値による共有鍵生成方式が有効であることが示されている．このことから，無線 LAN チップが異なっても本手法は有用であると考えるが，本手法の実用化の観点から，デバイスが異なることが，共通鍵生成にどのように影響を与えるかを検証する必要がある．

端末の位置関係と端末の振り方：本論文では，送信端末と受信端末の位置関係は一定とし，図 3 で示す一定の振り方で評価を行った．しかし，端末の位置関係やその振り方は，共通鍵を生成することに大きく影響すると考えられ，実環境では，これらを一定として扱うことは難しい．端末の位置関係やその振り方が共通鍵生成に与える影響について今後詳細に検証する必要がある．

使用チャネル：本評価では，2.4 GHz 帯でなく 5 GHz 帯の無線 LAN を利用した．2.4 GHz 帯は，電化製品などで使用されており雑音が多く，水に吸収されやすいために人体の影響を受けると考えられる．また，5 GHz 帯に比べ波長が長いために，伝送路の変化が生じにくいことも考えられる．実際に 2.4 GHz 帯で 4.1 節で述べた事前実験と同様に 10 回測定を行ったが，そのときの正規の送受信間の相関係数の平均は 0.88 であった．**図 18** に示すように，十分に相関は高いものの，5 GHz 帯を使用したときに比べると若干低下している．今後，2.4 GHz 帯での詳細な性能評価を進める必要がある．

6. おわりに

本研究では，近距離無線通信の暗号化通信に着目し，マルチパスの伝送路可逆性とフェージングの原理を用いて，共通鍵を配送することなく，同一の共通鍵を送受信端末間で生成する方式を提案した．提案方式では，小型端末に着目し，送信端末を振ることにより生じる無線伝送路の変動から共通鍵を生成する．また，提案手法を実環境により評価し，特別なデバイスを用いなくても，端末を振ることに注目することで，文献 [6] で提案された方式と比べて，盗聴されにくく，より高速に共通鍵を生成できることを確認した．特にバンドパスフィルタの適用により，盗聴が困難なマルチパス変動の情報を効率良く抽出できることを確認した．また評価結果から，パラメータを調整することで，誤り訂正符号による訂正なしでも，約 3 秒以内に 128 bit の共通鍵を約 95%以上の精度で送受信端末間で生成できることを確認した．

今後の課題としては，5.4 節で述べたものに加えて，以下があげられる．

- 生成した共通鍵のランダム性の評価として，0 と 1 の発生確率以外の観点（2 値行列ランク検定や DFT 検定などの観点）からの評価
- 共通鍵の品質を向上させる符号化方法の開発
- 使用チャネル，パケット送信間隔などが，共通鍵生成に与える影響への検証
- 人ごみや，雨が降っている環境などの雑音が大きな環境，また，マルチパスの反射がほとんどない環境，車や電車などの移動体の中など，様々な場所での検証
- 正規の送受信者の位置関係，および，そのときの振り方が共通鍵生成に与える影響への検証
- 様々な端末，および PC カードでの提案手法の評価
- 提案手法で利用するパラメータの値を自動的にチューニングする手法の確立

参考文献

[1] Aono, T., Higuchi, K., Ohira, T., Komiyama, B. and Sasaoka, H.: Wireless secret key generation exploitingreactance-domain scalar response of multipath fading channels, *IEEE Trans. Antennas and Propagation*, Vol.53, No.11, pp.3776–3784 (2005).
[2] 西野太志，笹岡秀一，岩井誠人：複数アンテナ送受信システムにおける電波伝搬特性に基づく秘密鍵共有方式（移動通信ワークショップ），電子情報通信学会技術研究報告，RCS，無線通信システム，Vol.108, No.445, pp.373–378 (2009).
[3] 角 武憲, 北浦明人, 立花 啓, 岩井誠人, 笹岡秀一：UWB 方式における遅延プロファイルに基づく秘密鍵共有方式，電子情報通信学会技術研究報告，無線通信システム，Vol.105, No.240, pp.19–24 (2008).
[4] 北浦明人：陸上移動通信における OFDM の伝送路特性に基づく秘密鍵共有方式，電子情報通信学会論文誌 A，Vol.87, No.10, pp.1320–1328 (2004).
[5] Mathur, S., Trappe, W., Mandayam, N., Ye, C. and Reznik, A.: Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel, *Proc. 14th ACM International Conference on Mobile Computing and Networking* (*MobiCom 2008*), pp.128–139 (2008).
[6] Jana, S., Premnath, S., Clark, M., Kasera, S., Patwari, N. and Krishnamurthy, S.: On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments, *Proc. 15th Annual International Conference on Mobile Computing and Networking* (*MobiCom 2009*), pp.321–332 (2009).
[7] Hershey, J.E., Hassan, A.A. and Yarlagadda, R.: Un-

conventional cryptographic keying variable management, *IEEE Trans. Communications*, Vol.43, No.1, pp.3–6 (1995).
[8] Tope, M.A. and McEachen, J.C.: Unconditionally securecommunications over fading channels, *Proc. Military Communications Conference* (*MILCOM 2001*), Vol.1, pp.54–58 (2001).
[9] Azimi-Sadjadi, B., Kiayias, A., Mercado, A. and Yener, B.: Robust key generation from signal envelopes in wireless networks, *Proc. 14th ACM Conference on Computer and Communications Security* (*CCS 2007*), pp.401–410 (2007).
[10] Bichler, D., Stromberg, G., Huemer, M. and Lw, M.: Key Generation Based on Acceleration Data of Shaking Processes, *Proc. Int'l Conf. Ubiquitous Computing* (*UbiComp 2007*), pp.304–317 (2007).
[11] 南 貴博，仁野裕一，野田 潤，中村嘉隆，関 浩之：ユーザの動作類似度に基づく共通鍵生成法，情報処理学会研究報告 マルチメディア通信と分散処理研究会報告，Vol.2009, No.20, pp.307–312 (2009).
[12] Hashimoto, T., Itoh, T., Ueba, M., Iwai, H., Sasaoka, H., Kobara, K. and Imai, H.: Comparative studies in key disagreement correction process on wireless key agreement system, *Computer Science Information Security Applications Lecture Notes in Computer Science*, Vol.4867, pp.173–187 (2007).
[13] Shimizu, T., Iwai, H. and Sasaoka, H.: Information Reconciliation Using Reliability in Secret Key Agreement Scheme with ESPAR Antenna, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Vol.17, pp.148–159 (2009).
[14] 川村俊一，清水崇之，岩井誠司，笹岡秀一：エスパアンテナを用いた秘密鍵共有方式における鍵容量の場所依存性，電子情報通信学会技術研究報告，RCS，無線通信システム，Vol.109, No.105, RCS2009–34, pp.37–42 (2009).
[15] 清水崇之，岩井誠司，笹岡秀一：エスパアンテナを用いた秘密鍵共有方式における盗聴耐性向上の検討，電子情報通信学会技術研究報告，A・P，アンテナ・伝播，Vol.108, No.148, AP2008–43, pp.41–46 (2008).
[16] NIST, FIPS PUB 197, Advanced Encryption Standard (AES) (2001).

推薦文

本研究は，安全なデータ通信を実現するうえで必要な共通鍵（共有情報）の共有を，送受信端末で個別に生成することで実現する手法を提案している．提案手法の主なアイデアは，送受信端末を振ることにより生じる無線伝送路の変動をもとにして，各端末で個別に共有情報を生成することにあり，有用性が高いため推薦する．

（ユビキタスコンピューティングシステム研究会主査 椎尾一郎）

岩本 智裕

2006 年九州大学工学部電気情報工学科卒業．同大学大学院システム情報科学府情報知能工学専攻修士課程在籍中．ET ロボコン九州大会総合優勝および学生ベスト理解容易モデリング賞受賞（2009 年）．ET ロボコンチャンピオンシップ大会にて審査員特別賞（2009 年），DICOMO 最優秀プレゼンテーション賞および優秀論文賞（2010 年），MoMuC 若手研究奨励賞（2010 年），九州大学学生後援会学術研究賞（2010 年）．モバイル・ユビキタスコンピューティング，ソフトウェア工学の研究に従事．

田頭 茂明 （正会員）

1996 年龍谷大学理工学部電子情報学科卒業．1998 年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了．2000 年同大学情報科学研究科博士後期課程修了．博士（工学）．2000 年広島大学工学部助手．2007 年同大学大学院工学研究科助教．同年九州大学高等研究院特別准教授，および同大学大学院システム情報科学研究院特任准教授．モバイル・ユビキタスコンピューティング，システムソフトウェアの研究に従事．本学会山下記念研究賞（2009 年），電子情報通信学会通信ソサイエティ活動功労賞受賞（2009 年）．IEEE，電子情報通信学会各会員．

荒川 豊 （正会員）

1977 年生．2001 年慶應義塾大学理工学部情報工学科卒業．2003 年同大学大学院修士課程修了．2004 年同大学 COE 研究員．2006 年同大学大学院博士課程修了．博士（工学）．2006 年同大学院特別研究助手．2007 年同大学院特別研究助教．2009 年 3 月より九州大学大学院システム情報科学研究院助教．2010 年 4 月より同大学システム LSI 研究センター助教（兼務）．2011 年 11 月より ENSEEIHT（フランス）訪問研究員．2012 年 2 月より DFKI（ドイツ）訪問研究員．主として，コンテキストアウェアなネットワークアプリケーション，およびそのデータマイニングに関する研究に従事．APCC 2008 Best Paper Award（2008 年），情報処理学会 MBL 研究会優秀論文賞（2009 年），DICOMO 優秀論文賞および優秀プレゼンテーション賞（2010 年），Mashup Award 6 GeoHack 賞および沖電気工業賞（2010 年），情報処理学会山下記念研究賞（2011 年），第 3 回フクオカ Ruby 大賞奨励賞（2011 年）．第 24 回安藤博記念学術奨励賞（2011 年），IEEE，電子情報通信学会各会員．

福田 晃 （フェロー）

1977 年九州大学工学部情報工学科卒業．1979 年同大学大学院工学研究科修士課程情報工学専攻修了．同年日本電信電話公社（現 NTT）武蔵野電気通信研究所入所．1983 年九州大学助手．1989 年同大学助教授．1994 年奈良先端科学技術大学院大学教授．2001 年九州大学大学院システム情報科学研究院教授，2008 年九州大学システム LSI 研究センター長（兼任），現在に至る．工学博士．組込みソフトウェア，ユビキタスコンピューティングに関する研究に従事．情報処理学会研究賞（1990 年），Best Author 賞（1993 年）等を受賞．情報処理学会フェロー，電子情報通信学会，ACM，IEEE Computer Society，日本 OR 学会各会員，「NPO 法人　九州組込みソフトウェアコンソーシアム（QUEST）」理事長．