様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月　 ６ 日現在

機関番号：３４３１０
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ０４０４８

研究課題名（和文）マルチパスフェージングの局所性を超える遠地点伝搬特性推定技術の開発

研究課題名（英文）Development of an estimation technique of distant propagation characteristics beyond locality of multipath fading

研究代表者
岩井　誠人（Iwai, Hisato）

同志社大学・理工学部・教授

研究者番号：７０４１１０６４

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：本研究では、無線セキュリティへの応用を目的として、伝搬特性の局所性を突破する技術の開発を目指した。その実現技術として、アレーアンテナに圧縮センシングによる信号処理を組み合わせた方式を検討した。圧縮センシングの処理における閾値設定を改良し、マルチキャリア信号を用いた場合の性能評価を行った。その結果、マルチキャリア信号を用いた場合には、フェージング環境の相関距離を大きく超える約35波長まで推定可能であることを示した。また、無線セキュリティ技術に関して、空間選択性変調方式、および、量子化符号語不一致低減と誤り訂正符号を併用する秘密鍵共有方式を提案し、それらの性能を明らかにした。

研究成果の学術的意義や社会的意義
無線通信のセキュリティを実現する技術の一つとして伝搬特性を利用した無線セキュリティ技術がある。この技術は、フェージング環境の伝搬特性の局所性を原理的基盤としている。本研究で検討した技術が実現されれば、このようなセキュリティ技術に対してより容易に盗聴が可能となる。セキュリティ技術の性能向上には、本研究で対象とする方式のような高度な盗聴方式を実現し、その対策技術を検討することが重要である。

研究成果の概要（英文）：This study aimed to develop a technique to destroy the locality of propagation characteristics for application to wireless security. As an enabling technology, a method combining array antennas with signal processing by compressed sensing was investigated. We improved the threshold setting in the processing of the compressed sensing and evaluated its performance when multi-carrier signals were used. As a result, it was shown that the system can estimate up to about 35 wavelengths, which greatly exceeds the correlation distance in a fading environment, when a multi-carrier signal is used. Regarding wireless security technology, we proposed a spatial selective modulation scheme and a secret key agreement scheme that combines quantization code word disagreement reduction and error correction codes, and clarified their performance.

研究分野：無線通信システムにおける電波伝搬

キーワード：電波伝搬　無線セキュリティ　圧縮センシング　到来方向推定　空間選択性変調　無線秘密鍵共有　レイトレーシング

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

無線通信システム、特に移動通信システムにおいて一般的であるマルチパスフェージング環境では、電波伝搬特性に「局所性」がある。複数電波が多方向から到来し、それが相互に干渉しあうことにより受信信号強度や位相などの伝搬特性に空間的な変動が生じる。その変動のスケールはフェージング変動が高相関となる限界距離である相関距離によって表される。相関距離は全周から一様の確率で電波が到来する環境では 1 波長(たとえば 5GHz で 6cm)以下であり、高い周波数では極めて短距離となる。このようなマルチパスフェージング環境の特徴を「伝搬特性の局所性」と呼ぶ。ある受信点から相関距離以上離れた遠方地点の伝搬特性はその受信信号と無相関となるため、推定することが困難である。

一方、この局所性を逆に活用した各種電波応用技術が複数提案されていた。その一つとして無線伝搬路の局所性および相反性に基づく秘密鍵共有技術があった。無線伝搬路はその送受信を逆としても受信側で得られる伝搬路は基本的に同一である。この伝搬路を情報源とみなした場合、その情報は、伝搬路の局所性のために送受信点でのみ共有可能なものとなる。これを暗号鍵生成に応用したものが無線秘密鍵共有方式である。

２．研究の目的

本研究では、上記の伝搬特性の局所性、すなわち、伝搬特性推定の距離の限界を突破する新しい技術の検討を目的とする。このような技術の実現により、たとえば無線秘密鍵共有方式では、より遠方地点からの秘密鍵盗聴が可能となる。その盗聴特性を定量的に評価し、その改善策を検討することはこのようなセキュリティ技術の性能を改善するためには重要である。そのためにはまず本推定技術のような技術の検討が必要となる。研究担当者は、それまでに無線伝搬路特性に基づくセキュリティ技術に関する研究を行ってきた。その検討の一つに、秘密鍵共有方式がある。本研究で提案する技術は、秘密鍵共有方式に対するアタック耐性を評価する中でその着想を得た。冒頭に述べたように一般的な単一アンテナ受信では相関距離を超えるアタックは実現できない。それに対して、アレーアンテナと信号処理を組み合わせることにより、相関距離を超える地点からでも秘密情報を得ることができるのではないかと考えた。これが本研究のきっかけである。本推定技術は無線セキュリティ技術にとっては盗聴行為の性能向上であり、研究として自己矛盾をはらんでいるとも言えるが、セキュリティ技術の性能の向上には、より高度な盗聴方式を想定しその対策技術を講じることが重要であり、無線セキュリティにとっても重要と考えた。

３．研究の方法

本研究では、遠方地点での伝搬特性推定を実現する方式として、アレーアンテナ構成の受信システムにマルチパスを構成する各到来波の到来方向推定および複素振幅推定を組み合わせる方式を検討した。推定方法は、アレー信号処理において到来方向推定などに用いられる圧縮センシングに基づく信号処理を用いる。この方式の推定性能を、計算機シミュレーションおよび室内実験により評価した。

推定の基本的な原理は、まず複数の波源位置(マルチパスフェージング環境では反射を考慮した鏡像波源位置)およびその波源の励振信号の複素振幅を、アレーアンテナ各素子の受信信号から推定する。その後、各波源から推定対象点に到達する受信信号を球面波などの仮定に基づいて求め、複数到来波の合成として最終的な受信信号(=伝搬特性)を推定する。

４．研究成果

目的を達成する技術について、過去の同目的の検討では、MUSIC 法による到来方向推定と最小二乗法による各波源信号の複素振幅推定を組み合わせた方式を用いていた。これを、本研究では、圧縮センシング方式の一つである FISTA を用いる方式へと変更した。これは、到来方向推定と複素振幅推定を一つの処理で行えること、マルチパスフェージングを対象とした場合には相関信号が対象となるが MUSIC 法は相関信号への対応に課題があること、FISTA の推定処理が比較的シンプルであること、などのメリットがあるからである。

検討すべき課題としては、環境変化に対する性能評価、球面波への対応、三次元環境への対応、が挙げられた。本研究では、その中の、球面波への対応について重点的に検討した。環境変化に対する性能評価は、到来波数やその方向、また、推定対象点までの距離、などの種々のパラメータが変化した際の推定特性を分析することによって結果を示した。三次元環境への対応については、二次元で実現された方式は三次元環境でも基本的にそのまま適用可能であり大きな課題は無いと考えられる。

球面波への対応は、まず、平面波環境の推定を単純に距離方向に拡張する方法を検討した。つまり、平面波環境では波源位置として到来方向のみの推定であるが、これを、到来方向と距離の二次元領域を対象とする推定方式に拡張した。しかしながらこの方法では、伝搬距離に伴って強度が低下する遠方波源からの到来波が検出困難であるという課題があることが明らかとなっ

た。そこで、FISTA の処理の閾値を波源位置までの距離に応じて変化させる方法を考案し、それにより推定性能を改善した。図 1 は、その結果の一例を示している。半波長間隔 20 素子のリニアアレーアンテナを用いて、3 波源(それぞれ波源 A,B,C とする。波源までの距離：15$\lambda$～50$\lambda$、角度：ボアサイトから±60 °、の範囲でそれぞれランダムに配置)のマルチパス環境において波源位置を推定した場合の、波源位置推定誤差の累積分布(CDF)を示したものである。遠地点伝搬特性推定の基となる、波源位置推定の精度が改善されていることがわかる。

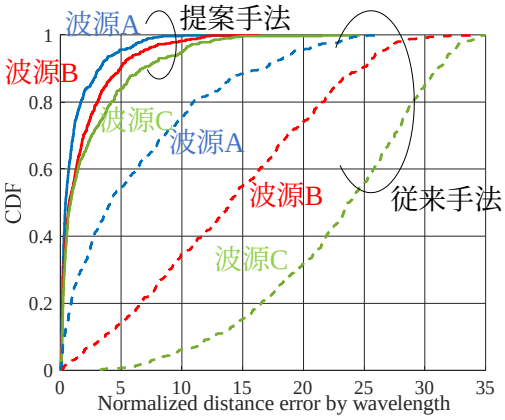

図1 推定波源位置誤差のCDF

上記の方法に加えて、さらなる推定精度の向上を目指し、対象信号をマルチキャリア信号とした場合の検討を行った。図 2 はその結果を示している。キャリア間隔$\Delta f$ の $N$ 個の周波数$f_n=f_0+n\Delta f(n=1,\ldots,N)$のマルチキャリア信号とし、$f_0$=5GHz、$N$=10 として、帯域幅を変化させた場合の結果である。同図は、原点から推定対象点までの距離に対する受信信号推定誤差($\varepsilon$)の RMS 値の変化を示している。同図より、近傍に比べて遠方地点の推定誤差は増加するが、帯域幅の増加に伴いより遠方での推定が可能となることがわかる。冒頭に述べた全周から一様に電波が到来するフェージング環境の相関距離は 1 波長以下(正確には 1/4 波長程度)であるが、たとえば帯域幅が 20MHz の場合には誤差 1dB 以下の推定が約 35 波長まで実現されている。このように、マルチキャリア信号を用いるシステムでは、遠方地点の伝搬特性を推定可能であることを示した。

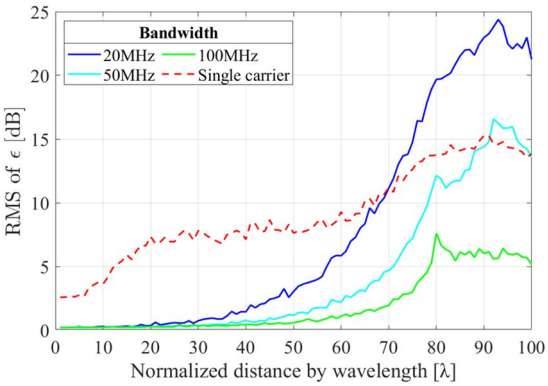

図2 推定対象点までの距離に対する推定誤差の変化

実際のマルチパスフェージング環境は、建物壁面などによる反射波によって構成されることとなる。これまで、対象とする環境は複数の異なる位置の波源から相関がある電波が送信されるという仮想的な環境を想定していたが、現実的な伝搬環境の具体例として室内環境を想定し、レイトレーシング計算によりマルチパス環境における伝搬路を求めることにより伝搬環境を計算する方法を導入した。図 3 はその結果の一例を示している。10m×8m の部屋を想定し、点(1,1)に推定用 20 素子アレーを円形に配置している。(2.6,0.6)から(9.4,7.4)に至る正方形エリアを波源を想定する領域として解析対象とした。解析対象各位置に波源が、部屋全体に推定対象点が、存在すると想定した場合の、推定受信信号強度の RMSE をカラーマップとして示している。多くの地点で推定誤差の RMSE は 1dB 以下となっている。解析対象全位置の RMSE は 1.73dB であり、マルチパスフェージング環境でも済遠地点伝搬特性推定が実現できることを示した。

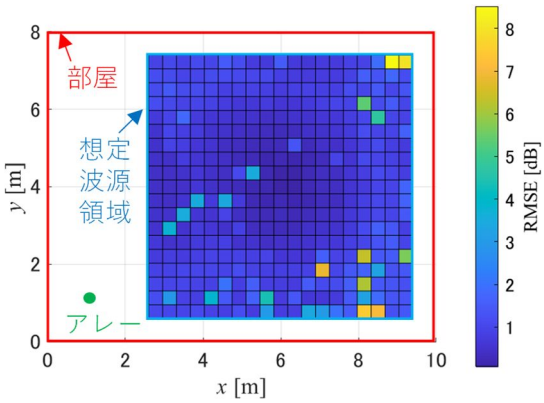

図3 室内環境を想定した場合の推定特性

また、遠地点伝搬特性推定技術によって攻撃(盗聴)される側の無線セキュリティ技術に関しても検討を進めた。その一例として、複数アンテナから定振幅の正弦波を送信し、その位相を送受信点間のチャネル特性に基づいて制御することにより、正規受信局位置でのみ信号を受信可能とする空間選択性変調方式について、盗聴耐性の評価を行った。その評価の中で、多数アンテナからより盗聴耐性の高いアンテナを選択的に使用する新しい方法を明らかにし、それによりセキュリティ性能が改善されることを示した。さらに、秘密鍵共有方式において、量子化符号語の不一致低減と誤り訂正技術による不一致訂正をバランスよく併用する新しい鍵不一致訂正技術を提案し、その性能を定量的に評価した。評価の結果、たとえば SNR14dB 以上の範囲において鍵不一致率 $10^{-3}$ 以下を達成できることを示し、高い鍵一致割合と鍵生成効率の両立が可能であることを示した。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　1件）

| | |
|---|---|
| １．著者名<br>Yonawa Hiroto、Iwai Hisato、Ibi Shinsuke | ４．巻<br>12 |
| ２．論文標題<br>Analysis of spatial distribution of secret transmission performance of SSM using ray-tracing | ５．発行年<br>2023年 |
| ３．雑誌名<br>IEICE Communications Express | ６．最初と最後の頁<br>305～310 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/comex.2023SPL0007 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>與縄 洋斗、岩井 誠人、衣斐 信介 | ４．巻<br>64 |
| ２．論文標題<br>室内環境における空間選択性変調方式の盗聴耐性に関する分析 | ５．発行年<br>2023年 |
| ３．雑誌名<br>同志社大学ハリス理化学研究報告 | ６．最初と最後の頁<br>59～69 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.14988/00029716 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>吉田正樹、笹岡秀一、岩井誠人、衣斐信介 | ４．巻<br>J107-B |
| ２．論文標題<br>適応量子化符号語を用いた無線物理層秘密鍵共有における符号語の不一致訂正と誤り訂正符号の併用による鍵一致に関する検討 | ５．発行年<br>2024年 |
| ３．雑誌名<br>電子情報通信学会論文誌 B | ６．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.14923/transcomj.2023JBP3034 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　1件）

| |
|---|
| １．発表者名<br>與縄洋斗、森嶋佑香、岩井誠人、衣斐信介 |
| ２．発表標題<br>室内環境における空間選択性変調方式の秘密伝送性能の評価 |
| ３．学会等名<br>電子情報通信学会　アンテナ・伝播研究会 |
| ４．発表年<br>2022年 |

１．発表者名
原一真、岩井誠人、衣斐信介

２．発表標題
圧縮センシングによる到来角度・距離の二次元推定における距離推定の性能改善

３．学会等名
電子情報通信学会　アンテナ・伝播研究会

４．発表年
2022年

１．発表者名
Hiroto Yonawa, Hisato Iwai and Shinsuke Ibi

２．発表標題
Evaluation of Secret Transmission Performance of Spatially Selective Modulation

３．学会等名
2022 International Symposium on Antennas and Propagation (ISAP2022)（国際学会）

４．発表年
2022年

１．発表者名
原一真，岩井誠人，衣斐信介

２．発表標題
マルチパスフェージング環境における遠地点受信信号推定

３．学会等名
電子情報通信学会関西支部第26回学生会研究発表講演会

４．発表年
2022年

１．発表者名
大黒佐輔、岩井誠人、衣斐信介

２．発表標題
送信アンテナ選択によるSSMの耐盗聴性能の改善

３．学会等名
電子情報通信学会アンテナ・伝播研究専門委員会

４．発表年
2023年

| |
|---|
| １．発表者名<br>大黒佐輔、岩井誠人、衣斐信介 |
| ２．発表標題<br>送信アンテナ選択によるSSMの耐盗聴性能の改善 |
| ３．学会等名<br>電子情報通信学会ソサイエティ大会 |
| ４．発表年<br>2023年 |

| |
|---|
| １．発表者名<br>山田大翔、原一真、岩井誠人、衣斐信介 |
| ２．発表標題<br>マルチキャリア信号を対象とした圧縮センシングによる遠地点受信信号推定 |
| ３．学会等名<br>電子情報通信学会関西支部第28回学生会研究発表講演会 |
| ４．発表年<br>2024年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|