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 ２４ 日現在

機関番号：２０１０６
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ０４４６３

研究課題名（和文）mMTCシステムでの情報理論的安全な鍵共有を目指した分散無線通信方式の検討

研究課題名（英文）A study of distributed wireless communications aiming for information theoretic secured key sharing in mMTC systems

研究代表者
高野　泰洋（Takano, Yasuhiro）

公立千歳科学技術大学・理工学部・准教授

研究者番号：７０７８２７４６

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究は，mMTCシステムでの情報理論的安全な鍵共有を目指し，当該無線伝送方式と，そこで必要となるパラメータ推定法について検討した．具体的には，mMTCネットワークに配備された安価なIoT受信端末に対してもセキュア伝送を実現可能な送信プリコーディング技術を提案した．また，現実的な伝送系でセキュア伝送を実現するためには制約付き最適化問題を繰り返し実行する必要があるが，その高速化を提案した．更に，鍵生成パラメータをAIで推定した場合の脆弱性を調査するため，回帰ベースの到来方向推定法および測位法を提案し，その推定性能を実伝搬環境で検証した．

研究成果の学術的意義や社会的意義
本研究が提案した制約付き最適化問題の高速化手法はSignal-to-noise ratio (SNR) に依らず一定の処理時間で実行可能であり，多数ノードを有するmMTCシステムでのセキュア伝送の実現に向けて有意義である．また，AIを応用した従来のパラメータ推定法の多くは分類アルゴリズムである．しかし，チャネルパラメータに基づく鍵情報の元になる乱数を生成する際，量子化されたパラメータ推定値を用いることはランダム性を損なう懸念がある．これに対し，提案した回帰ベースのAIアルゴリズムは連続値を出力するため，ランダム性の問題を改善することができる．

研究成果の概要（英文）：We study secure transmission protocols and the required estimation techniques under the aim of assuring the information theoretic security for key-sharing in massive machine type communication (mMTC) system. Specifically, we proposed a new transmission precoding technique to perform secure transmission for low-cost IoT terminals dispatched in mMTC networks. Additionally, a low-complexity solver algorithm is proposed to improve complexity issues that can be happened in iteratively performing regularized optimization. Furthermore, in order to investigate vulnerabilities for key parameters estimated by AI-based techniques, new AI-aided regression algorithms for direction of arrival (DoA) estimation and localization techniques are proposed and verified in real propagation channels.

研究分野：情報通信工学

キーワード：Physical layer security　Regularized optimization　SLNR-based Tx precoding　MMSE-based Tx precoding　Compressed sensing　CNN regularion　Bi-LSTM regularization

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Internet-of-Things（IoT）ネットワーク基盤の構築が進みつつあるが，中でも，多数の通信ノードで構成される massive Machine Type Communication（mMTC）システムでは強固にセキュアな情報伝送が求められている．従来，暗号化によってセキュリティが保証されてきたが，ハードウェアの性能向上や暗号解析技術の進歩を考慮すると，未来永劫，安全性が保証されるとは限らない．そこで安全性向上を目指し，物理チャネルの統計的な性質を利用した物理層セキュリティ（PLS）が注目を集めている．PLS は，Massive Multiple-Input Multiple-Output（MIMO）システムでの高精度な Beamforming 技術や Artificial Noise（AN）伝送により，正規ユーザー間と傍聴者間との通信リンクの通信容量を制御して，情報理論的安全性を統計的に達成可能である．PLS では，鍵を必要としないが，その安全性強度はチャネルの状態に大きく依存するため，チャネルパラメータの解析が重要な課題の一つである．

２．研究の目的

本研究は，mMTC システムでの情報理論的安全な鍵共有を目指し，当該無線通信方式と，そこで必要となるパラメータ推定法について検討する．また，近年，Artificial Intelligence（AI）アルゴリズムによるパラメータ推定法が従来法に比べ推定精度を改善する事例が報告されている．これらのアルゴリズムが攻撃に利用されうることを考慮し，本研究は，AI を応用したパラメータ推定器を実装し，計算機シミュレーションおよび実伝搬系により性能検証する．更に，情報理論的安全性と計算量的安全性を併せ持つフレームワークについて調査する．

３．研究の方法

a）圧縮センシングを応用した情報理論的安全な無線伝送の検討

情報理論的安全な無線伝送は，Beamforming と AN 伝送を活用して送信元でリンク間のチャネル容量差で定義される Secrecy Capacity を制御することで実現される．Beamforming や AN 伝送はチャネルパラメータに依存するため，PLS の実現には，チャネル推定精度の向上およびそれを考慮した適応的な送信制御法が不可欠である．この問題は Secrecy Capacity 最大化の最適化問題として形式化されるが，本研究は，安価な IoT 受信端末に対してもセキュア伝送を実現可能な送信プリコーディングを検討する．次に，分散ネットワークでは制約条件の増加および解の探索範囲の増加といった，問題の複雑性が高まる懸念がある．そこで，本研究は軽量な最適化手法も検討する．

b)鍵情報共有に関する安全性の検討

PLS の情報理論的安全性はチャネルパラメータの統計的な性質に依存する．一方，分散ネットワークを構成する全ての無線リンクで所望のパラメータ特性が保証されるとは限らない．そこで本研究は，セキュア伝送機能の可用性を保証するため，PLS と従来の暗号化を組み合わせた鍵の配布方法が必要である．PLS に基づく鍵共有のアプローチの一つとして，正規の通信者間で共有されるチャネルパラメータに基づき，鍵の生成情報を共有する手法が知られている．近年，AI アルゴリズムによるパラメータ推定器が従来の統計的なアプローチに基づく推定器より推定誤差を改善する場合があることが報告されている．これは正規の通信者間での鍵共有の通信レートを改善しうる．しかし，AI が出力するパラメータ推定値を活用することで新たな脆弱性が発生しうる．あるいは，分散ネットワークにおいて，不特定の敵が AI を利用して鍵の生成情報を傍聴することも懸念される．そこで，鍵情報共有に関する安全性検討の課題の一つとして，AI を応用したパラメータ推定器を実装し，計算機シミュレーションにより性能検証する．

c）実伝搬環境における鍵生成パラメータ共有の予備実験

従来の統計的信号処理に基づくパラメータ推定法が実行困難となりうる伝搬シナリオであっても，訓練データが与えられれば AI ベースの推定法が実行可能なことがある．そこで，鍵生成パラメータ共有を目指し，本研究では，ソフトウェア無線機や商用 Wi-Fi 端末を利用し，実伝搬環境におけるパラメータ推定法を検討し，実検証する．

d）計算量的安全性と情報理論的安全性を統合するフレームワークの調査

従来の暗号化と PLS を組み合わせたセキュリティに関し，その理論体系はまだ十分に検討されていない．そこで，本研究は計算量的安全性と情報理論的安全性を統合するフレームワークを調査し，今後の展望を検討する．

４．研究成果

a）圧縮センシングを応用した分散ネットワークでの情報理論的安全な無線伝送

分散ネットワークでは，ノードが流動的にネットワークへ接続，切断しうるため，そのノード数が既知とは限らない．この課題に動機づけられ，ユーザー数が未知である mmWave 伝送系におけるブラインドチャネル推定法[5]を提案した．具体的には，基地局の受信信号の相関行列のランク数を解析し，ユーザー数を推定する．その後，圧縮センシングのアプローチを利用し有意なパスの到来方向の推定する．提案法は分散ネットワークでのチャネル推定にも応用できる．

次に，Signal-to-leakage-and-noise ratio (SLNR)規範に基づく送信プリコーディングは低中 Signal-to-noise ratio (SNR)領域において,セキュア伝送を実現可能なことが知られているが,従来法は受信端末がチャネル推定および等化を実行する必要があった.そこで本研究は,安価な IoT 端末がチャネル推定および等化処理を実行することなくセキュア伝送を実現できるように，SLNR に加え Minimum mean square error (MMSE)の両規範に基づく適応的な送信プリコーディング技術[1]を提案した．図 1 に示す通り，提案の適応伝送法は,傍聴者の受信を妨げると同時に,固定レートのセキュア伝送に比べ有意にスループット性能を向上させる．

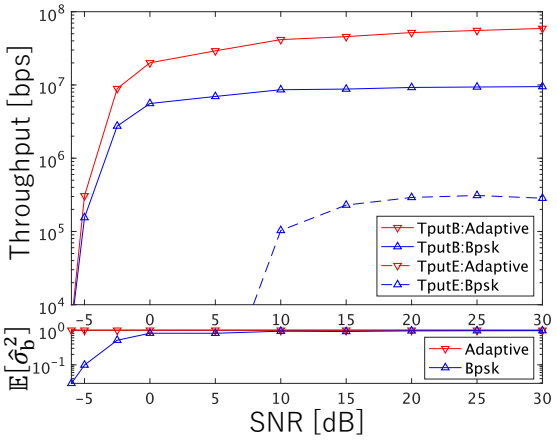

図 1 スループット性能

更に，現実的な伝送系で情報理論的安全な無線伝送を実現するためには，チャネル推定誤差による Capacity の劣化と変調アルファベットに応じた達成可能な伝送レートの上限を考慮した上で，Secrecy Capacity が最大になるように秘密情報と AN の最適な電力比を決定する必要がある．この制約付き最適化問題は，Logarithm barrier 法により解くことができる．しかし，想定する全ての変調アルファベットごとに当該手法を繰り返し実行する必要があるため，Logarithm barrier 法による演算量が増加してしまう．そこで，我々は[2]にて，キャッシュを利用した適応的セキュア伝送系のための電力最適化法を提案した．具体的には,Bisection により制約つき求根問題を解く．Bisection において，局所最適解への探索パスは 1/(2^n)の分解能で量子化される．また，最適化問題が実行不能であるとき，変調アルファベットに起因する制約条件に依らず，量子化された解の探索パスが近似的に同一になる．図 2 に示す通り，提案法(C-bisect)はキャッシュに保存された局所最適解への探索パスを参照することで，セキュア伝送の実行に不適切な変調アルファベットを高速に判別し，最適化問題全体の演算量を有意に削減した．

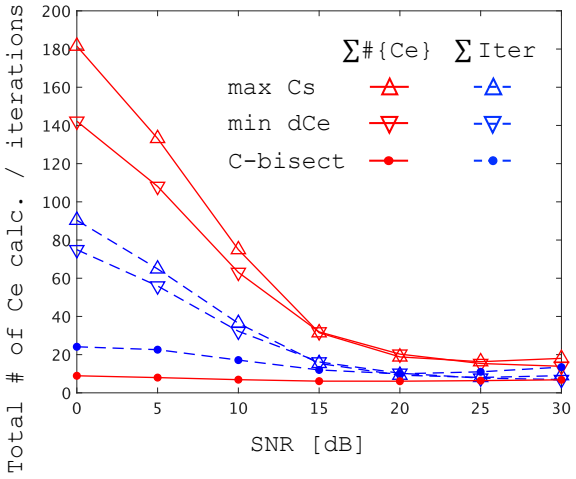

図 2 計算量の収束特性

b) 鍵情報共有を目指した AI に基づくパラメータ推定法の検討

本研究は，AI を応用したパラメータ推定器として，Bi-directional long short term memory (Bi-LSTM)回帰を用いた Direction of Arrival (DoA)推定器[3]を提案した．狭帯域フェージングチャネルを想定した計算機シミュレーションでは，CNN 分類法に比べ，提案法は低 SNR 領域において有意な Mean squared error (MSE)ゲインを得る．複数の信号源が独立に時間変動する場合，従来の Root-MUSIC 法に比べて，Bi-LSTM 回帰は低中 SNR 領域において有意な MSE ゲインを達成する．しかしながら，当該時間変動シナリオにおいて，最善の性能を達成しうる Bi-LSTM 回帰は 0.1 度のオーダーで MSE フロアが見られ，Cramer-Rao 限界から乖離することを確認した．これらの結果は，鍵情報として DoA を用いた場合の量子化誤差の指標を与える．また，本研究は，関連する課題として，非均一アレイ構造をもつハイブリッドビームフォーミングシステムの性能を解析した[5]．具体的には，推定すべき信号源の数が RF チェーンの数より多い劣決定問題を非均一アレイ構造により改善することを提案した．分散ネットワークではノード間の協調により，非均一アレイ構造を想定できる．そこで，今後の展望として，本研究は[3]と[6]のアプローチ組み合わせた AI に基づくパラメータ推定法を検討し，当該技法を応用した鍵共有アルゴリズムの安全性を検証する．

c) 実伝搬環境における鍵生成パラメータ共有の予備実験
鍵生成パラメータ共有を目指し，本研究は，実伝搬系におけるパラメータ推定を検証した．具体的には,Convolutional neural network (CNN)回帰を用いたReceive signal strength indicator (RSSI)測位法[4]を提案した．RSSIに基づく最も基本的な測位法として，フリスの伝達公式に基づく三辺測量が挙げられる．しかし，非線形性を有する屋内の伝搬環境において，三辺測量は実用的な推定性能を達成できない．10m x 10mのテスト領域において，絶対誤差(MAE)の評価実験において，提案のCNN回帰は，従来のK近傍(KNN)法のそれの53%であるMAE=1.7mを達成することを検証した.ここで,従来の機械学習を応用した推定器は分類ベースのアルゴリズムであるが,提案法はb),c)共に回帰ベースのアルゴリズムである．このことは，チャネルパラメータに基づく鍵情報の元になる乱数を生成する際，量子化された推定値を用いることでランダム性を損なう懸念がある．これに対し，提案した回帰ベースのAIアルゴリズムは連続値を出力するため，ランダム性の問題を改善することができる．更に，実伝搬環境での実験結果から，非線形性を伴うチャネル情報と位置情報との間に有意な相関があること確かめられた．今後の展望として，本研究は[4]で得られた知見に基づき，位置情報に基づくセキュア伝送法を検討する．

d) 計算量的安全性と情報理論的安全性を統合するフレームワークの調査
本研究は，これまでBell Laboratories Layer Space-Time (BLAST)ベースのセキュア伝送システムを検討してきた．しかし，文献調査の結果，Spatial Shift Keying (SSK) や Precoding-aided Spatial Modulation (PSM) 等もセキュア伝送を実現する有望なフレームワークとして注目されていることが判った． MIMO系での送受信アンテナの組み合わせの部分集合を利用するこれらのフレームワークでは，従来の伝送シンボルに加え，送信または受信アンテナのインデックスも利用したアルファベットにより情報を表現する．つまり，全ての組み合わせを探索可能であるためアンテナインデックスによる情報表現は計算量的安全性を保証する．一方，同時に伝送する従来のシンボルデータは，セキュア伝送の原理に従ってプリコーディングされれば，情報理論的安全性を達成しうる．今後の展望として，本研究は，SSKやPSMといった計算量的安全性と情報理論的安全性を併せ持つフレームワークについて，それらのSecrecy Capacity性能や攻撃耐性について検討を進める．

主要論文

[1] Y. Takano and H.-J. Su, "A Joint SLNR-MMSE-based Adaptive Secure Transmission Technique for Broadband IoT Systems," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322201.

[2] Y. Takano, H.-J. Su, Y. Shiraishi and M. Morii, "A Cache-Aided Power Optimization Technique for Adaptive Secure Transmission Systems," 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 2022, pp. 1122-1127, doi: 10.1109/PIMRC54779.2022.9978041.

[3] H. Inoue, Y. Takano, H.-J. Su, and S. Ozawa, "A Bi-LSTM Regression-Aided Estimation Technique for Time-Varying Multiple DoAs," 2024 9th International Conference on Business and Industrial Research (ICBIR), accepted for publication on 2024/03/14.

[4] R. Muraguchi, Y. Takano, and H.-J. Su, "An RSSI Indoor Localization Technique Using CNN Regression, " Proceedings of the 2023 12th International Conference on Networks, Communication and Computing, pp. 80-84, doi: 10.1145/3638837.3638849.

[5] Y.-T. Hou, H.-J. Su and Y. Takano, "Blind Channel Estimation for Millimeter Wave Uplink Systems with Unknown Number of Users," 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan, 2022, pp. 445-450, doi: 10.1109/PIMRC54779.2022.9978006.

[6] Y.-C. Liu, H.-J. Su and Y. Takano, "Underdetermined AOA Estimation of Correlated Sources Using Hybrid Beamforming Based on NSC Structure," 2023 IEEE Globecom Workshops (GC Wkshps), Kuala Lumpur, Malaysia, 2023, pp. 805-810, doi: 10.1109/GCWkshps58843.2023.10464484.

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　9件／うちオープンアクセス　1件）

１．著者名 Takano Yasuhiro、Su Hsuan-Jung、Shiraishi Yoshiaki、Morii Masakatu	４．巻 2022
２．論文標題 A Cache-Aided Power Optimization Technique for Adaptive Secure Transmission Systems	５．発行年 2022年
３．雑誌名 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan.	６．最初と最後の頁 1122-1127
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/PIMRC54779.2022.9978041	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Hou Yi-Ting、Su Hsuan-Jung、Takano Yasuhiro	４．巻 2022
２．論文標題 Blind Channel Estimation for Millimeter Wave Uplink Systems with Unknown Number of Users	５．発行年 2022年
３．雑誌名 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Kyoto, Japan.	６．最初と最後の頁 445-450
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/PIMRC54779.2022.9978006	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Liu Yu-Chen、Su Hsuan-Jung、Takano Yasuhiro	４．巻 2022
２．論文標題 Enhanced Multiple Angles-of-Arrival Detection Using Non-uniform Sub-connection in Hybrid Beamforming Systems	５．発行年 2022年
３．雑誌名 2022 IEEE Globecom Workshops (GC Wkshps), Rio de Janeiro, Brazil.	６．最初と最後の頁 13-18
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/GCWkshps56602.2022.10008613	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Takano Yasuhiro、Su Hsuan-Jung	４．巻 -
２．論文標題 A Joint SLNR-MMSE-based Adaptive Secure Transmission Technique for Broadband IoT Systems	５．発行年 2020年
３．雑誌名 GLOBECOM 2020 - 2020 IEEE Global Communications Conference	６．最初と最後の頁 1-6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/GLOBECOM42002.2020.9322201	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Liu Chu-Tung、Su Hsuan-Jung、Takano Yasuhiro	4．巻 -
2．論文標題 Sparse Activity, Timing Detection and Channel Estimation for Grant-Free Uplink Communications	5．発行年 2020年
3．雑誌名 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications	6．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/PIMRC48278.2020.9217319	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Lai Ting-Wei、Su Hsuan-Jung、Liu Chu-Tung、Takano Yasuhiro	4．巻 -
2．論文標題 Resource Allocation of Multi-Cell Full-Duplex Networks Based on Ant Colony Optimization	5．発行年 2020年
3．雑誌名 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications	6．最初と最後の頁 1-7
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/PIMRC48278.2020.9217194	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Liu Hsiang-Yu、Su Hsuan-Jung、Takano Yasuhiro	4．巻 -
2．論文標題 Deep Learning-Aided NOMA Codebook Design with Improved Performance	5．発行年 2023年
3．雑誌名 2023 XXXVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS)	6．最初と最後の頁 1-4
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/URSIGASS57860.2023.10265593	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Muraguchi Reiya、Takano Yasuhiro、Su Hsuan-Jung	4．巻 -
2．論文標題 An RSSI Indoor Localization Technique Using CNN Regression	5．発行年 2023年
3．雑誌名 Proceedings of the 2023 12th International Conference on Networks, Communication and Computing	6．最初と最後の頁 80-84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3638837.3638849	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Haruta Inoue, Takano Yasuhiro, Su Hsuan-Jung, Ozawa Seiichi	４．巻 -
２．論文標題 A Bi-LSTM Regression-Aided Estimation Technique for Time-Varying Multiple DoAs	５．発行年 2024年
３．雑誌名 2024 9th International Conference on Business and Industrial Research (ICBIR)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス 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 該当する

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 高野泰洋，白石善明，森井昌克
２．発表標題 無線セキュア伝送の研究動向調査
３．学会等名 コンピュータセキュリティシンポジウム 2020 (CSS 2020)
４．発表年 2020年

１．発表者名 Inoue Haruta、Takano Yasuhiro、Su Hsuan-Jung、Ozawa Seiichi
２．発表標題 Performance Verification of DoA Estimation for MUSIC-like Statistical-based and LSTM Classification-based Algorithms
３．学会等名 Chitose International Forum 2023（国際学会）
４．発表年 2023年

１．発表者名 Muraguchi Reiya、Takano Yasuhiro、Su Hsuan-Jung
２．発表標題 Performance Verification of a KNN-based RSSI Localization
３．学会等名 Chitose International Forum 2023（国際学会）
４．発表年 2023年

１．発表者名
Fujita Kandai、Takano Yasuhiro、Su Hsuan-Jung

２．発表標題
A Survey on Deep Learning-based Channel Estimation Techniques

３．学会等名
Chitose International Forum 2023（国際学会）

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

2022年度第3回公開講座「情報セキュリティ往古来今」
https://snc.chitose.ac.jp/archives/4476.html
准教授・博士（情報科学）、理学博士（工学）：高野 泰洋
https://www.chitose.ac.jp/course/teacher/539

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （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			
その他の国・地域（台湾）	National Taiwan University			