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　３ 年　 ５ 月 ３１ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ０６４２３

研究課題名（和文）物理層セキュリティに注目した情報理論的安全な第５世代移動通信システム

研究課題名（英文）An Information-theoretic secured 5G mobile communications system utilizing physical layer security

研究代表者
高野　泰洋（TAKANO, Yasuhiro）

神戸大学・工学研究科・助教

研究者番号：７０７８２７４６

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：５G移動通信システムでは10Gbps以上の伝送速度を達成する一方，傍聴者への情報漏洩も懸念される．通信の安全性強化のため，従来の暗号化に加え大規模MIMO 伝送の空間自由度を活用し情報理論的安全性を達成しうる物理層セキュリティの実現が期待されている．しかし，その性能はチャネル推定精度に大きく依存する．
この問題の解決策として，圧縮センシング，ターボ受信，そして独立主成分分析の概念に基づく時空間-部分空間法を利用した新たな推定法を示した．更に，これらのパラメータ解析を活用し，IoT端末向けの堅牢なセキュア伝送法を提案した．今後の課題として，なりすまし耐性をもつ応用プロトコルを精査する．

研究成果の学術的意義や社会的意義
先行研究の多くはチャネルパラメータが既知と想定していたが，当該パラメータは推定すべきである．また，推定誤差を考慮したセキュア伝送法はまだ十分に議論されていなかった．本研究は，まず，大規模MIMOでのPilot汚染，未知干渉問題に対する根本解決策を示した．そして，Uplink-Downlink Duality仮定に誤差があっても堅牢にセキュア伝送を実現する新たな通信法を提案した．安価なIoTセンサ端末に対しても有意な秘匿チャネル容量を達成する提案法は，Society 5.0における安全なIoTネットワーク構築のための基盤技術の一つとして活用が期待される．

研究成果の概要（英文）：5G mobile communication systems have a risk of information leakage to eavesdroppers while achieving transmission (Tx) ratio more than 10Gbps. In addition to the conventional cryptography, the physical layer security (PLS) that can achieve information theoretic security by leveraging spatial degree of freedom in massive MIMO is expected to improve the risk. However, performance of the PLS depends significantly on the channel estimation accuracy.
As a solution to the problem, we show new estimation techniques by exploiting compressive sensing, turbo receiving and spatial-temporal subspace-based approaches based on the concept of the independent component analysis. Moreover, we proposed a new robust secure Tx method for IoT terminals by exploiting the above-mentioned estimation techniques. Future study is to verify protocols using the secure Tx method against spoofing attacks.

研究分野：情報通信工学

キーワード：physical layer security　secure transmission　Internet of things (IoT)　turbo channel estimation　compressive sensing　subspace-based method　ICA　SLNR

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

第５世代(5G)移動通信システムでは大規模 MIMO 伝送やミリ波帯域を利用して 10Gbps 以上の伝送速度を目指している．伝送速度向上は，正規通信者間では利便性をもたらすが，一方，傍聴者へ漏洩する情報量も増加しうる．このことは，これまで無線通信の安全性は計算量的安全性に基づく暗号化技法により保証されてきたが，漏洩情報量の増加に伴い Ciphertext-only-attack (COA) 等攻撃の危険性を高める．一方，5G システムでの新たなセキュリティ技術として，大規模 MIMO 伝送の高い空間自由度を使ったチャネル・レシプロシティ(CR)による情報理論的安全な物理層伝送が可能になる．その実現に向け活発に研究が進められているが，多くの先行研究ではチャネルを既知と想定していた．しかし，無線通信ではチャネルは推定すべきパラメータである．特に，セキュア伝送では，Artificial Noise (AN) による安全性向上が想定されているため，未知干渉下での MIMO チャネル推定技術は必須である．ところが，大規模 MIMO 系において当該技術は未だ十分に議論されていなかった．また，CR 性能はチャネル推定精度に依存するため，当該推定誤差を補償もしくは許容するセキュア伝送技法の確立が望まれていた．

２．研究の目的

５G 移動通信の安全性向上を目的とし，本研究は，情報理論的安全性を達成しうる物理層セキュリティ技術を検討する．具体的には，物理層セキュリティの一つのアプローチである CR によるセキュア伝送法について，まず前提技術であるチャネル推定法の性能向上に取り組み，大規模 MIMO における CR 伝送実現に向け課題抽出とその理論的性能を明らかにする．そして，チャネル推定誤差を補償もしくは許容するセキュア伝送技法の確立を目指す．更に，CR にて懸念されるなりすまし攻撃の対策案を検討する．

３．研究の方法

a) 大規模 MIMO 系でのチャネル推定性能向上:

大規模 MIMO 系は，数十から数百の送受信アンテナによって得られる空間的自由度により，高精度なチャネルパラメータ与えられれば，通信容量向上が期待できる．一方，直交性を持つパイロット信号を用いてチャネル推定は実行されるが，有限長系列から理想的な直交性を持つパイロット信号群を生成することは困難である．従って，大規模 MIMO では伝送ストリーム数の増加に伴い直交性の損なわれたパイロット信号がチャネル推定精度劣化を招く「Pilot 汚染」問題が生じる．本研究は，この Pilot 汚染を再現する MIMO 伝送シミュレーション実験環境を構築する．そして，「系列長/(送信ストリーム数 ＊ 推定すべきパラメータ数)」で定義される比率 Rpc に応じて Pilot 汚染によりチャネル推定精度が劣化することに注目し，その改善策を検討する．またその理論的性能を明らかにする．

b) チャネル推定誤差を補償もしくは許容するセキュア伝送技法の確立:

CR 伝送は，一般的に，Time division duplex (TDD)を想定し，Uplink と Downlink のチャネルパラメータが同一である(UL-DL duality)と仮定する．そして，CR は，Uplink で推定したチャネルパラメータを利用し，Downlink の送信重み行列を算出する．従って，CR の伝送性能はチャネル推定精度に依存する．また，送信間隔が必ずしも短期間ではない現実的な通信系では，当該 UL-DL duality 仮定が成り立つとは限らない．つまり，理想的なチャネル推定値を得ても，CR 性能が劣化する懸念がある．そこで，上記課題 a)にて理論的に解析したチャネル推定性能に基づき，チャネル推定誤差および UL-DL duality 誤差を補償もしくは許容する CR 伝送を検討する．

c) なりすまし攻撃の対策:

CR 伝送は次の２段階の手順で構成される：①正規の通信者 Bob による UL Request (Pilot 信号の伝送)後，基地局 Alice がチャネル推定および送信重みを算出し，②Alice による DL Acknowledgement (Bob の Request 承認および秘密情報の送信)．しかし，一般的な CR 伝送法は，手順①の通信者が本当に Bob であるか確認しないため，悪意のある第３者 Eve により「なりすまし攻撃」を被る懸念がある．そこで，本研究は，なりすまし攻撃の耐性を持つ CR 伝送のための通信プロトコルを検討する．

４．研究成果

a) チャネル推定の性能向上：

Pilot 汚染は上記比率 Rpc に応じて伝送性能の劣化を招く．従って，a-1)系列長を増加させる，a-2)推定すべきパラメータ数を減少させる，といったアプローチにより問題改善できる．本研究は，アプローチ a-1)としてターボチャネル推定に注目した．ターボチャネル推定は，Pilot 系列に加え，Data 部の復号器出力の Loglikelihood ratio (LLR)を利用して参照信号長を増加させることが可能である．ターボチャネル推定は，Pilot 部と Data 部に関する同時最尤推定問題として形式化され，その解はテンソル積の逆行列算出のため高い演算量を必要としていた．本研究は，下記主要論文[4]で提案したとおり，テンソル積を含む共分散行列の代数的特徴に着目し，演算精度を損なうことなく高速実行可能なアルゴリズムを示した．次に，圧縮センシングにより

アプローチ a-2)に取り組み，Inter-block interference 問題に対するターボチャネル推定の性能向上(主要論文[3])を実現した．更に，圧縮センシングと Independent component analysis (ICA)の概念を応用し，時空間-部分空間法に基づくチャネル推定法(主要論文[2])を提案し，当該技法が未知干渉 MIMO チャネルでの推定性能を有意に改善することを検証した．

b) セキュア伝送の堅牢性向上:
既存のセキュア伝送法は，傍聴者への情報漏洩量を最小にするよう設計されていたが，DL 受信時にチャネル推定と等化処理が必要だった．このため，本研究は，当初，チャネル長と秘匿容量の関係を解析(学会発表[RCS2019/01])し，DL 送信時に短い Pilot を送信し，Bob のみが正常に受信できるプロトコルを検討していた．しかし，当該 DL Pilot の利用は Eve の傍聴成功率を高めてしまう．そこで，上記成果 a)のチャネル推定の解析的性能を活用して，DL Pilot 伝送を必要としない新たなセキュア伝送法を提案した．主要論文[1]に示したとおり，Bob の受信信号に関して Signal-to-leakage-and-noise ratio (SLNR)と Minimum mean square error (MMSE)の同時規範問題を形式化し，Subspace 法を応用しこの解を導出した．これにより，DL 受信機は単にゲイン調整のみで秘密情報を受け取ることができる．主要論文[1]では，提案法の秘匿チャネル容量およびスループット性能を評価し，送信間隔が長い IoT 系における安価なセンサ端末に対してもセキュア伝送が可能なことを検証した．

c) なりすまし攻撃の対策:
学会発表[CSS2017]にて，CR 伝送に認証フェーズを追加したプロトコルを議論した．また，主要論文[5]では，ブロックチェーンに事前登録された情報を活用した認証プロトコルを提案した．ブロックチェーン上の情報を活用することで，認証手続きの簡素化を図ると同時に，ハッシュ関数の不可逆性による対改竄性を論理的に検証した．今後の課題として，当該プロトコルを利用した CR 伝送について改竄耐性およびスループット性能を精査する．

主要論文

[1] Y. Takano and H.-J. Su, "A Joint SLNR-MMSE-based Adaptive Secure Transmission Technique for Broadband IoT Systems," IEEE GLOBECOM 2020, pp. 1-6.

[2] Y. Takano, H.-J. Su, Y. Shiraishi and M. Morii, "A Spatial-Temporal Subspace-Based Compressive Channel Estimation Technique in Unknown Interference MIMO Channels," IEEE Trans. Signal Proc., vol. 68, pp. 300-313, 2020.

[3] Y. Takano, H. -J. Su, M. Juntti and T. Matsumoto, "A Conditional ℓ1 Regularized MMSE Channel Estimation Technique for IBI Channels," IEEE Trans. Wireless Commun., vol. 17, no. 10, pp. 6720-6734, Oct. 2018.

[4] Y. Takano and H.-J. Su, "A Low-Complexity LS Turbo Channel Estimation Technique for MU-MIMO Systems," in IEEE Signal Proc. Lett., vol. 25, no. 5, pp. 710-714, May 2018.

[5] T. Tsuchida, M. Takita, Y. Shiraishi, M. Mohri, Y. Takano, and M. Morii, "Authentication Scheme Using Pre-Registered Information on Blockchain," IEICE Trans. on Information and Systems, 2019, Vol. E102.D, No. 9, pp.1676-1678, Sep. 2019.

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　8件／うち国際共著　7件／うちオープンアクセス　0件）

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 Takano Yasuhiro、Su Hsuan-Jung、Shiraishi Yoshiaki、Morii Masakatu	４．巻 68
２．論文標題 A Spatial--Temporal Subspace-Based Compressive Channel Estimation Technique in Unknown Interference MIMO Channels	５．発行年 2020年
３．雑誌名 IEEE Transactions on Signal Processing	６．最初と最後の頁 300～313
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TSP.2019.2959223	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 Lin Jhe-Yi、Su Hsuan-Jung、Hong Chen-Chieh、Takano Yasuhiro	４．巻 -
２．論文標題 Low Complexity Hybrid Precoder Design for mmWave Multi-User MIMO Systems: A Non-Iterative Approach	５．発行年 2019年
３．雑誌名 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)	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/VTCFall.2019.8891355	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 Wang Wei-Hsiang、Su Hsuan-Jung、Takano Yasuhiro	４．巻 -
２．論文標題 Performance Analysis of MU-MIMO Systems with Threshold-based Feedback and Spatial Heterogeneity	５．発行年 2019年
３．雑誌名 2019 IEEE Wireless Communications and Networking Conference (WCNC)	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/WCNC.2019.8885514	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、Juntti Markku、Matsumoto Tad	4．巻 17
2．論文標題 A Conditional L1 Regularized MMSE Channel Estimation Technique for IBI Channels	5．発行年 2018年
3．雑誌名 IEEE Transactions on Wireless Communications	6．最初と最後の頁 6720～6734
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TWC.2018.2863295	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 25
2．論文標題 A Low-Complexity LS Turbo Channel Estimation Technique for MU-MIMO Systems	5．発行年 2018年
3．雑誌名 IEEE Signal Processing Letters	6．最初と最後の頁 710～714
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LSP.2018.2820811	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 1
2．論文標題 Performance of frequency domain multiuser-MIMO turbo equalization without cyclic prefix	5．発行年 2017年
3．雑誌名 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)	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/PIMRC.2017.8292314	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 TSUCHIDA Toshiki、TAKITA Makoto、SHIRAISHI Yoshiaki、MOHRI Masami、TAKANO Yasuhiro、MORII Masakatu	4．巻 E102.D
2．論文標題 Authentication Scheme Using Pre-Registered Information on Blockchain	5．発行年 2019年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1676～1678
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018OFL0005	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 －

〔学会発表〕　計11件（うち招待講演　2件／うち国際学会　3件）

1．発表者名
Takano Yasuhiro、Su Hsuan-Jung

2．発表標題
A Joint SLNR-MMSE-based Adaptive Secure Transmission Technique for Broadband IoT Systems

3．学会等名
IEEE Globecom 2020（国際学会）

4．発表年
2020年

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（CSS2020）

4．発表年
2020年

1．発表者名
高野泰洋

2．発表標題
時空間-部分空間圧縮チャネル推定を利用したMIMO伝送性能

3．学会等名
IEICE Tech. report, vol. 119, no. 448. Mar. 2020

4．発表年
2020年

1．発表者名
高野泰洋

2．発表標題
圧縮チャネル推定の研究動向

3．学会等名
IEICE Tech. report, vol. 119, no. 378. Jan. 2020

4．発表年
2020年

１．発表者名
Takano Yasuhiro、Su Hsuan-Jung

２．発表標題
A low-complexity LS turbo channel estimation technique for MU-MIMO systems

３．学会等名
IEEE Global SIP 2018（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
高野 泰洋, 白石 善明, 森井 昌克,

２．発表標題
秘匿伝送を想定した大規模MIMO システムにおけるターボチャネル推定法の高速化

３．学会等名
2018信学ソ大（基礎・境界）

４．発表年
2018年

１．発表者名
高野 泰洋

２．発表標題
条件付きL1正規化チャネル推定法を用いた物理層セキュリティの検討

３．学会等名
無線通信システム研究会（RCS）2019年1月

４．発表年
2019年

１．発表者名
Takano Yasuhiro、Su Hsuan-Jung

２．発表標題
Performance of frequency domain multiuser-MIMO turbo equalization without cyclic prefix

３．学会等名
2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017（国際学会）

４．発表年
2017年

１．発表者名
高野泰洋，白石善明，森井昌克

２．発表標題
線物理層セキュリティを用いたIoTネットワークの検討

３．学会等名
コンピュータセキュリティシンポジウム(CSS2017)

４．発表年
2017年

１．発表者名
Takano Yasuhiro

２．発表標題
An Introduction to MMSE Channel Estimation Techniques

３．学会等名
電気関係学会関西連合大会 2017（招待講演）

４．発表年
2017年

１．発表者名
土田敏生，瀧田愼，古本啓祐，白石善明，高野泰洋，毛利公美， 森井昌克

２．発表標題
グループ暗号通信のためのマルチホップ無線ネットワーク上での分散秘密の配付

３．学会等名
電気関係学会関西連合大会 2017

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
神戸大学 情報通信研究室 ES3
http://www.research.kobe-u.ac.jp/eng-es3/index.html

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
研究協力者	ＨｓｕａｎーＪｕｎｇ　Ｓｕ (Hsuan-Jung Su)	国立台湾大学	
研究協力者	白石　善明 (SHIRAISHI Yoshiaki) (14501)	神戸大学	
研究協力者	森井　昌克 (MORII Masakatsu) (14501)	神戸大学	

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			
台湾	国立台湾大学			
フィンランド	オウル大学			