日本―ドイツ、ポーランド 国際共同研究「レジリエント、安全、セキュアな社会のための ICT」 2021 年度　年次報告書	
研究課題名（和文）	高信頼かつ頑健な分散型 AI アルゴリズムの開発と応用 (TRURL)
研究課題名（英文）	Trustworthy Distributed Learning (TRURL)
日本側研究代表者氏名	湯川　正裕
所属・役職	慶應義塾大学・准教授
研究期間	2021 年 4 月 1 日～2024 年 3 月 31 日

１．日本側の研究実施体制

氏名	所属機関・部局・役職	役割
湯川　正裕	慶應義塾大学 理工学部 准教授	研究総括、アルゴリズム設計・解析
山田　功	東京工業大学 工学院 教授	研究総括、アルゴリズム設計
山岸　昌夫	東京工業大学 工学院 助教	アルゴリズム設計・解析、数値実験

２．日本側研究チームの研究目標及び計画概要

当該年度の第一目標は、スパース信号に対する分散型オンライン推定法の開発であり、弱凸正則化関数を導入することで、高い推定精度を達成しながら、大域的最適解への収束が保証された分散型アルゴリズムを構築する。第二目標は、DDoS 攻撃検出のための高精度ロバスト主成分分析の開発であり、DDoS 攻撃の特徴をより精密に表現した凸関数の最小化戦略を採用することで、高精度な DDoS 攻撃検出法を構築する。

3. 日本側研究チームの実施概要

2021 年度に実施した研究の概要を簡潔に記す。

1. ミニマックス凹型罰則関数に基づく分散型最適化アルゴリズムの構築

ミニマックス凹型罰則項（minimax concave penalty）に基づく分散型最適化アルゴリズムを構築し、大域的最適解への収束を保証するための条件について検討した。以下、2 つの主要成果について簡潔に記す。

成果 1. ミニマックス凹型罰則項をそのままの形で用いた場合、局所関数の凸性を担保できないことが明らかになった。そのため、入力ベクトルの独立性に基づく近似を導入することで、局所関数の凸性を保証する「近似型ミニマックス凹型罰則項(Approximate Minimax Concave Penalty)」を提案し、その有効性を実証した。本成果は、7 月に開催された IEEE Statistical Signal Processing Workshop 2021 におけるスペシャルセッション（Signal Modelling, Adaptive Learning and Applications）で発表済である。

成果 2. 成果 1 で述べた近似型ミニマックス凹型罰則項は、入力ベクトルの独立性の仮定が成り立たない状況で性能が劣化することが確認された。そのため、近似を用いない手法として、合意促進罰則(Consensus Promoting Penalty)関数の導入を提案した。合意促進罰則関数は、合意部分空間上で零値を取り、その直交補空間上で強凸性を持つ。対照的に、データから決まる損失関数は合意部分空間上で強凸性を持つ。これにより、損失関数に、ミニマックス凹型罰則項と合意促進関数を同時に加えることで、ミニマックス凹型罰則項の持つ弱凸性（特別な非凸性）が打ち消され、目的関数全体が凸関数になることをシミュレーションで実証した。さらに、目的関数が凸関数であるための必要条件を明らかにした。合意促進罰則関数の導入により、大域的最適解への収束が保証できるだけでなく、収束速度が大きく改善されることを明らかにした。本成果は、この夏に開催予定の国際会議 European Signal Processing Conference (EUSIPCO) 2022 に採択された。

以上、2 つの研究成果をまとめた論文は、国際学術ジャーナル IEEE Transactions on Signal and Information Processing over Networks への掲載が決定している（2022 年 5 月 22 日採録決定）。以上の成果は、慶應大・TUB チーム（ドイツ）の共同研究成果である。

2. 異常通信検出の精度向上に向けた行列近似分解モデル(cLiGME モデル)の構築

ネットワークの異常検出問題に対する信号処理的アプローチとしてネットワークトモグラフィー[Vardi, 1996]が知られている。ネットワークトモグラフィーは、比較的容易に観測可能な通信トラヒック情報から構成されたデータ行列（拡大 OD フロー行列）を異常通信に起因する行列成分と正常通信に起因する行列成分の和に近似分解することにより、異常通信発生を顕在化させる基本戦略に基づいた信号処理手法と見ることができる。

東工大チームでは、ネットワークトモグラフィーの数理モデルを進化させることにより、異常通信分析性能を向上させることを目標としており、拡大 OD フロー行列の分解性能を左右する「正則化項付き最小 2 乗推定モデル」を現代的視点から見直すと共に、新世代の行列近似分解モデルとその解法アルゴリズムの実現に挑戦している。

2021 年度は、異常通信/正常通信の特徴付けの鍵となる「非負行列のスパース性」や「非負行列の低ランク性」の近似評価尺度を飛躍的に向上させる「行列近似分解モデル(cLiGME モデル)」を構築することに成功している。cLiGME モデルは、信号処理分野で強力な汎用解法となってきた「Set-theoretic estimation」の機能を丸ごと LiGME 型最小 2 乗推定モデル[Abe, Yamagishi, Yamada, Inverse Problems, 2020]に組込んだ革新的な「正則化項付き最小 2 乗推定モデル」である。東工大チームでは、cLiGME モデルを、DDoS 攻撃を想定したネットワークトモグラフィーに応用し、課題の洗い出しも行っている。