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」 2023 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・教授
研究期間	2021 年 4 月 1 日～ 2025 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・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	法政大学・理工学部・准教授	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、分位点回帰に基づく分散型オンライン非線形関数推定法の開発であり、スパース推定のための分散型アルゴリズムと融合させることで、信頼性の高い推定法を構築する。第二目標は、悪意のあるクライアントによる攻撃（ビザンチン攻撃）に頑健な連合学習アルゴリズムの開発である。第三目標は、LiGME モデル[Abe et al., Inv. Probl., 2020]に基づく分散型アルゴリズムの開発であり、分散型 RPCA によって DDoS 攻撃を高精度に検出する数理的枠組みの構築を目指す。

3. 日本側研究チームの実施概要

日本側研究チームの実施概要を以下、簡潔に記す。

1. 慶応大とドイツチームの連携により、２つの研究課題に取り組んだ。第一課題は、「誤りデータを除外したロバスト分位点回帰法」である。センサー故障等の原因で生じた「本当の値と大きく異なるデータ（外れ値と区別して、便宜上、誤りデータと呼ぶ）」が不特定な割合で混入している場合に対して、「信頼できるデータ（誤りデータ以外）」のみから分位点を推定する問題に取り組んだ。提案法は、ピンボール損失関数と MC（Minimax Concave）罰則関数を合成した「左右非対称な」MC 関数を定義し、誤りデータ以外のデータ（正常データ）の分位点を高精度に推定できることをシミュレーションで確認した。第二課題は、「共分散行列の推定誤差にロバストな角度パワースペクトル（APS）推定法」である。次世代移動体通信システムでは、多数のアンテナを搭載した大規模 MIMO システムが検討されている。しかし、アンテナ数が増加した場合、APS 推定に用いられる上り回線の共分散行列の推定に用いるサンプル数が相対的に小さくなり、サンプル共分散行列の精度が劣化する。そのため、従来の角度パワースペクトル推定法は、アンテナ数を増やしても、APS 推定の精度が向上しないという課題を抱えていた。本研究で提案する手法は、多カーネル適応フィルタに基づいており、APS の滑らかさを暗に仮定しているため、アンテナ数を増加させることで、推定精度を大きく改善できることが明らかになった。本研究成果を記した論文は、国際会議へ投稿済である。
2. 法政大チームは、クライアントの異常行動履歴に基づく信頼度評価のための評価基準を提案し、同基準を用いて、ビザンチン攻撃検出法とビザンチン攻撃を繰り返すクライアント検出法を提案した。具体的には、ビザンチン攻撃の代表例である sign-flipping 攻撃を想定し、通常のクライアントと攻撃者の応答の違いを利用して、コサイン類似度によって分類することで、多数決によって攻撃者を検出する戦略である。本研究では、同類似度基準を用いて、各時刻において各クライアントの応答の「攻撃らしさ」を定量化する評価基準を提案し、各応答が「攻撃であるか否か」を判別する手法を提案した。さらに、あるクライアントの（一定タイムスパンにおける）応答が一定以上の割合で攻撃と判定された場合に、そのクライアントを攻撃者と判定する手法を提案した。MNIST データセットを用いた手書数字画像の分類問題の連合学習における提案法の有効性を数値例で確認した。
3. 東工大チームは、DDOS 攻撃検出のための基盤技術であるロバスト主成分分析の高性能化に直結する四つの研究課題に取り組み、国際会議論文（IEEE ICASSP）4 編、国際学術論文誌掲載 4 編（内 1 編は電子情報通信学会論文賞受賞）など、大きな成果を得た。第一に、LiGME モデル（Abe, Yamagishi, Yamada 2020）に対して、一般の線形変換に適用可能な「代数的 GME 行列設計法」の実現に成功した。また、スパースな区分的定数信号の推定モデル(Latent fused lasso)の凸正則化を cLiGME による非凸正則化に置き換えた新モデルを提案した。第二に、DC 最適化アルゴリズムが抱えるインナーループの有限停止性を保証する世界初の近似 DC アルゴリズムを実現することに成功した他、DC 型非凸正則化モデルの代表例として scaled generalized minimax concave (sGMC)モデル（LASSO モデルの一般化）に注目し、その解集合の幾何学的性質と正則化経路解析を行い、sGMC モデルの正則化経路を有限回の計算で算出可能とするアルゴリズムを世界ではじめて実現した。これらに加えて、「正規直交制約付き平滑最適化のための適応 Cayley パラメータ表現法と収束性能解析」と「非凸制約付き非平滑最適化のための可変平滑化法とその応用」にも取り組み、大きな成果が得られた。