様式 1-4-2 (2019-1)

平成 30 年度研究開発成果概要書

採 択 番 号　　：19301
研究開発課題名 ：スマートコミュニティを支える高信頼ネットワーク構成技術の研究開発
副　　題　　：STEAM：スマートコミュニティを支えるエネルギーとモビリティを対象としたセキュアな高信頼フレームワーク

（1）研究開発の目的

本研究開発では、将来のスマートコミュニティ実現に不可欠な高度交通システムとスマートエネルギーシステムを対象に、安全性と信頼性を担保しながら、エッジコンピューティングでそれらのアプリケーションを実現する高信頼ネットワーク基盤の研究開発を行う。様々な脅威モデルのもとでも、アプリケーション意思決定プロセスの安全性・信頼性保証、および個々のデータプライバシー保護を実現する新しい計算スキームを提唱し、実用性の観点からセキュリティレベルと計算資源のトレードオフ問題を追求する。それらの機能を有するエッジコンピューティングミドルウェア基盤を開発し、アプリケーション実データを利用した都市スケールの有効性評価を行う。

（2）研究開発期間

平成３０年度から平成３３年度（３６ヶ月）

（3）実施機関

国立大学法人奈良先端科学技術大学院大学＜代表研究者＞
学校法人早稲田大学
国立大学法人大阪大学

（4）研究開発予算（契約額）

総額　　４５百万円（平成 30 年度　　９百万円）
※百万円未満切り上げ

（5）研究開発項目と担当

研究開発項目１：不確実性に対し堅牢かつ安全な意思決定方式の開発（参考）
１－１．異常検知技術（ミズーリ工科大学）
１－２．信頼モデル構築技術（ミズーリ工科大学）
１－３．意思決定モデル構築技術（ミズーリ工科大学）

研究開発項目２：プライバシー保護計算機構の開発
２－１．表探索によるプライバシー保護計算技術（早稲田大学）
２－２．範囲検索の実現技術（早稲田大学）
２－３．FHE および差分プライバシーによる異常検知技術（早稲田大学）

研究開発項目３：セキュリティ・プライバシーレベルと計算資源のトレードオフ解析（参考）
３－１．プライバシー制約のもとでの閾値決定手法（ヴァンダービルト大学）
３－２．動的状況のもとでの閾値決定手法（ヴァンダービルト大学）
３－３．暗号化を要するセンサーデータの決定手法（ヴァンダービルト大学）

研究開発項目４：統合ミドルウェア基盤の設計開発研究開発
４－１．「地産地処」分散計算と集約機構（奈良先端科学技術大学院大学）

４－２．通信と集約処理における匿名化機構（奈良先端科学技術大学院大学）
４－３．トレードオフを考慮した意思決定機構（大阪大学）

研究開発項目５：スマートコミュニティ応用事例による評価
５－１　マルチモーダル経路計画への応用と評価（大阪大学）
５－２　トランザクティブ・エネルギーへの応用と評価（ヴァンダービルト大学）

（6）特許出願、論文発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	1	1
	その他研究発表	4	4
	プレスリリース・報道	0	0
	展示会	0	0
	標準化提案	0	0

（7）具体的な実施内容と成果

■研究開発項目２：プライバシー保護計算機構の開発

完全準同型暗号を用いたプライバシー保護計算機構として、研究開発項目１で実施する異常検知計算を行うための手法について検討すると共に基本手法の開発を行った。具体的には、現在の完全準同型演算でサポートされている積和演算以外の計算を完全準同型暗号で実現する手法として、各種計算を表検索（Lookup Table）に置き換える手法を研究開発した。あらかじめ必要となる計算を関数として用意し、入力値と出力値を表に保存する。その上で、入力された入力値から表を探索し出力値を求める。

従来研究では、ビット演算を用いて表探索を行っていたのに対し、提案手法では、整数のままで表探索ができる手法を提案した。これによって、従来のビット演算による手法に比較して高速化を達成した。具体的には、従来研究では１回の表探索に１時間かかっていたものを 23 秒（27,000 個の 15bit 整数の表を用いた場合）に短縮（約１５０倍の高速化）することに成功した。さらに、並列処理（マルチスレッド処理）を適用することで６秒まで短縮した。

次に、上記の表探索は、あらかじめ表に用意されている入力値のみに対してしか出力を得ることができないことを改善するために、完全準同型暗号を用いた大小比較手法を研究開発した。従来の大小比較手法は（１）暗号化されている比較結果を一旦復号しないと後の演算（積）で使えない、もしくは（２）その適用できる整数の範囲に限定があり、実用的ではなかった。提案手法ではこれらの問題を解決し、扱うことのできる整数の範囲を拡大（130bit まで実験）でき、かつ、暗号化されている比較結果を復号せずに後の演算で利用できることを確認した。さらに、整数の範囲が 40bit 以下であれば、従来手法よりも高速（約 2.7 倍）であることを確認した。

以上、研究開発項目１の異常検知計算を完全準同型暗号で実行しプライバシー保護を行うための基本手法の開発を進めた。

■研究開発項目４：統合ミドルウェア基盤の設計開発研究開発

スマートメーターや EV 車両などからセキュアにデータを収集し、解析計算を行うエッジコンピューティングミドルウェアアーキテクチャの設計開発に関する基礎的な検討を行うとともに、ミドルウェアの初期プロトタイプを開発した。具体的には、セキュアで信頼できるミドルウェアアーキテクチャの機能要件を整理するとともに、各種データ処理における処理タスクを適切なサブタスク

に分割し、計算リソースや推定実行時間をベースに分散したエッジノードに柔軟に割り当てる機構の基本設計を行った。また、各種計算処理における将来の資源デマンドを推定する技術についての基礎検討を行った。さらに、エッジコンピューティング環境においてセンサーデータストリームの分散処理を行うミドルウェア技術を開発し、上記アーキテクチャにおけるデータストリームのリアルタイム処理機能を実現している。

成果として、資源管理、サービス連携、タスク実行からなるミドルウェアアーキテクチャを設計し、Docker を用いて初期プロトタイプを実装するとともに、オフィス空間におけるコンテキスト推定・クエリーサービスやスマートビルディングサービスに応用し、複数エッジノードへのタスクの分散により、ユーザからの同時発行クエリー数が増えても応答時間を一定時間内に抑制可能なことや、分散しない場合と比較し各エッジノードの負荷を 1/6 程度に抑制可能なことなどを確認した。

■研究開発項目５：スマートコミュニティ応用事例による評価

本グループが有する交通シミュレータを用いて、スマートモビリティシステムにおける移動経路計画実現のためのモビリティモデルの検討を行った。特にマルチモーダル経路計画における現実的な行動モデルを実現するための車両モビリティモデルを開発するとともに、日本の実環境における実際の渋滞や交通量を再現するために VICS データを活用してモビリティを決定するためのスキームを検討し、その初期プロトタイプを開発している。そのシミュレータをもとに交通速度や交通量取得を可能とする拡張を行い、異常検知と信頼性意思決定アルゴリズムを評価可能なシステムを開発する。

（8）外国の実施機関

ミズーリ工科大学（アメリカ）＜代表研究者＞
ヴァンダービルト大学（アメリカ）