様式 1-4-2 (2020-2)

令和２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年度から令和３年度（36 か月）

（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（令和２年度　　１５百万円）
※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．異常検知技術（ミズーリ工科大学）
2．信頼モデル構築技術（ミズーリ工科大学）
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

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．範囲検索の実現技術（早稲田大学）
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）

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）
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．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

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）
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）

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
１　マルチモーダル経路計画への応用と評価（大阪大学）
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、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	2	1
	その他研究発表	20	8
	標準化提案・採択	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	2	1

（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

2-2. 範囲検索の実現技術は、任意の関数実行を実際の計算をすることなくテーブル検索により代替する技術である。テーブルには予め入力値と出力値（事前計算済みの値）のペアが保存される。テーブルの入力値に完全一致しない値が関数の引数として入力された時、引数に最も近いテーブルの入力値を選択する手法を PIR（Private Information Retrieval：プライベート情報検索）を用い実装した。同インプリメントにより、任意の引数が与えられた場合も、テーブル検索により関数の出力を得ることができることを確認し、約 100 万個エントリを持つ表に対して 4.04 秒での処理（８スレッド実行時）を実現した。

2-3. FHE および差分プライバシーによる異常検知技術では、研究開発項目１で開発された手法を完全準同型（FHE）により実装し、テキサス州 200 家庭の 2014 年から 2016 年の電力消費データを用いて評価した。実装においては、除算を用いない新手法を提案し、計算過程において一度も復号化せずに実現した。結果、暗号化前と同精度での異常値検知を１０秒間隔で実現することに成功した。当初目標である数分内での実現が可能となったため、実行時間短縮を実現するための回避策として予定していた差分プライバシーは適用していない。

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においては、異常検知や信頼性決定モデル（項目１）を、プライバシー、セキュリティと資源のトレードオフ（項目３）を考慮しながら実現する仕組みを検討した。特に、FHE 計算におけるデータ集約はエッジサーバーにおいて多くの計算資源を消費することが分かっており、十分な資源がない場合はユーザーが許容できない遅延が生じる可能性があるため、適切なプライバシーレベルやセキュリティ/トラストレベルを定義し、高度なプライバシー保護を必要とするデータのみを保護する機構を検討した。また、米国側研究分担者の Dubey のグループが開発している、路側機（RSU）からなるネットワーク上での、エッジコンピューティングおよびフェデレーションラーニングを用いた最短時間経路の分散計算法と、奈良先端大のグループが開発している、多数の経路探索クエリーを RSU ネットワークにおいて分散処理するタスク割当方式を組み合わせ、本研究で開発しているミドルウェアのアプリケーションとして実装し、ナッシュビル市と大阪市の交通データを用いて評価を行った。

4-2．通信と集約処理における匿名化機構と 4-3．トレードオフを考慮した意思決定機構においては、分散経路探索を対象に、エッジコンピューティング環境においてプライバシーを保護しながらデータ送信・集約する以下の手法を考案しプロトタイプの開発を行った。

・秘匿性、整合性および可用性を満たしながら FHE 計算により復号プロセスを経ることなくデータを集約する手法として、Private Information Retrieval (PIR) と FHE を組み合わせた経路探索手法を考案した。

・経路探索において、PIR を適用する地理的範囲、交差点の数を変化させることで、プライバシ保護レベル、計算時間の短さ、計算結果の正確さの 3 つの指標間のトレードオフを考慮可能な方法を考案した。

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

5-1．マルチモーダル経路計画への応用と評価においては、歩行者と車両が混在する交通環境のモデル化とシミュレーション設定を行った。特に、大阪大学と協力関係にある豊岡市と連携し、豊岡市の観光地区におけるマルチモーダル交通状況をモデル化した。具体的には、同地区の主な市営駐車場４つに対する車両デマンドならびに歩行者デマンドを設定し、確率モデルを用いた経路計算を行うことで、同地区における歩行者と車両の交通流を再現した。また、多数の歩行者が道路上を移動することで車両の渋滞が発生する状況を現実に即して再現した。この手法を、以前より構築している大阪市シミュレーション環境に適用する計画である。

（8）今後の研究開発計画

令和３年度は、最終年度であるため、各研究開発項目において開発した個々の手法の有効性評価を行うと共に、研究開発を行った機能を統合することでエッジコンピューティングミドルウェア基盤を完成させ、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。

（9）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）
ウエスタンミシガン大学（アメリカ）