様式 1-4-2 (2021-1)

令和３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３年度７百万円）
※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、ウェスタンミシガン大学）
2. 信頼モデル構築技術（ミズーリ工科大学、ウェスタンミシガン大学）
3. 意思決定モデル構築技術（ミズーリ工科大学、ウェスタンミシガン大学）

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	3	1
	その他研究発表	23	3
	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	3	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

- 完全準同型暗号を用いたプライバシー保護計算機構を実現した。
- 研究開発項目 1 の成果への完全準同型暗号の適用方法として、「①スマートグリッド（パワーグリッド）に特化し、完全準同型暗号下での計算量を抑える手法」と「②アプリケーションによらず完全準同型暗号下での計算を表探索により可能とする手法」の２種類を開発した。
- 両手法をスマートグリッド（パワーグリッド）での異常検知に適用し、200 家庭の実電力使用量データに対する攻撃を 10 秒以内（①の方法）、５分以内（②の方法）に検知できることを確認した。スマートグリッド（パワーグリッド）を対象とした異常検知の要求条件は 1 時間毎の検知であり、本結果は要求条件を満たす。また、暗号を用いない場合と同等の異常検知精度を持つことを確認した。

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

- エッジノードの分散処理により、SCC アプリケーションを実行可能なミドルウェア基盤を開発した。本基盤は、これまで広域通信・クラウドでの処理が必要であった IoT システムをデータ発生源近くの IoT デバイスのみからなる分散システムにより実現することができること、局所的な計算需要の増加に対応するために、タスクの割当可能範囲を動的に拡張する「適応的スケールアウト」の機能を持つことが特徴である。
- ナッシュビル市道路網を 49 個のグリッドエリアに分割し（各グリッドに 1 台の RSU が設置されると想定）、49 個の Docker 仮想マシン上で実行するエミュレーション環境を PC 上に構築し、評価を行った。各 RSU は、対応するグリッド内の各道路の実交通データ（時間帯ごとの平均車速）を使って経路を算出する。本環境上で、2000 クエリに対しても 300 秒以下という実用可能な時間で処理可能なことを確認した。
- スマートモビリティアプリケーションを対象に、クエリの始点・終点を匿名化し、匿名化状態でルートを探索し、ユーザが結果を外部に知られることなく取得する手法（匿名分散ルート探索機構）と、を開発した。また、処理時間、プライバシー保護度合い、検索結果の正確さの３つの項目のトレードオフを考慮しながら最適なルート検索する多目的最適化問題を定式化し、NSGA-Ⅱ に基づくアルゴリズムを開発し、提案手法が既存の単一目的最適化アルゴリズムより優れていることを示した。
- 米国ナッシュビル市の各道路セグメントの時系列交通データ（時間帯ごとの平均車速）と天候データ、車両事故データからなるデータセットを構築し、時系列交通データから個々の事故（incident）を異常として検出する機構の開発を行った。

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

・広域における車両移動（広域モビリティ）を実現するための方法論を開発した。マルチモーダル経路計画への応用と評価においては、スマートトランスポートシステムにおける道路利用量に対する経路推定を行う手法を開発した。具体的には、リンク交通量を用いて OD マトリックスの推定を行う機械学習モデル（DNN、CNN、LSTM）を構築した。観測したリンク交通量から、事前に用意した 108 パターンの OD マトリックスの中で最も近いものを正確に分類できることが確認できた。

・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。具体的には、兵庫県豊岡市の観光地区において、同地区の主な市営駐車場 4 つに対する車両デマンド取得を行った。同市が保有するデータから、11 月のある休日における、駐車場における入退出データ、および、近くの主要道の交通トラフィックから同市に流入するトラフィックを解析した。同地区の観光客の周遊を再現するため、駐車場を始点および終点とする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い、同地区における歩行者と車両のマクロ交通流を再現した。以上により、車両移動、歩行移動が混在したモビリティの生成が可能になった。

（8）研究開発成果の展開・普及等に向けた計画・展望

・本研究では、エネルギーとモビリティを対象としたスマートコミュニティアプリケーションを安全安心に運用するための基礎技術の確立を目指し、FHE を用いたプライバシー保護機構、異常検知や信頼性決定をセキュリティと資源のトレードオフを考慮しながら実現する仕組みを組み込んだミドルウェア基盤を開発した。今後は、開発したミドルウェア基盤のライセンシング等の推進を検討していく。

・内閣府が推進する「スーパーシティ構想」により、今後、都市のスマートシティ化が加速していくと思われるが、既存の都市 OS は標準となるセキュリティ・プライバシー保護機構を持たないため、本研究開発の成果であるミドルウェア基盤と都市 OS の相互接続、統合を検討する。

・研究代表者・分担者らが連携している、京都スマートシティ推進協議会、生駒市、豊岡市等と協力し、実際の都市に提案基盤を適用していくことを検討する。

（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）
ウェスタンミシガン大学（アメリカ）