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　　：19101
研究開発課題名　：未来を創る新たなネットワーク基盤技術に関する研究開発
副　　題　　：IoT インタネットを支えるプライバシー保護ルーティング・輻輳制御技術

（1）研究開発の目的

本研究開発の目的は、プライバシー、IoT デバイスへのルーティング、輻輳制御などの問題を解決して、センサデータのプライバシーを保護しつつ、収集者が実時間でセンサデータを収集する事を可能とするクラウドソーシングに適したアーキテクチャを開発することである。本アーキテクチャの基盤技術は、プライバシー保護可能な属性ルーティング技術、及びキャッシュを利用したネットワーク主導のマルチパス輻輳制御技術である。これらを組み合わせて、5G 以降の多様な無線ネットワークから構成されるインタネットにおいて、あまねく設置された IoT デバイスから取得したセンサデータを、プライバシー情報を保護しつつ、オープンにアクセスできる IoT 時代のインタネットを実現することを目指す。

（2）研究開発期間

平成２８年度から令和２年度（５年間）

（3）実施機関

国立大学法人大阪大学 〈代表研究者〉
パナソニック株式会社

（4）研究開発予算（契約額）

総額　　１００百万円（令和２年度　２０百万円）
※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： プライバシーを保護する属性ルーティング
1. 属性ルーティング（パナソニック株式会社）
2. プライバシ保護ルーティング（大阪大学）

研究開発項目２： 実時間クラウドソーシングアプリケーション
1. アプリケーション設計（パナソニック株式会社）
2. マルチパス輻輳制御（大阪大学）

（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	7	1
	外国出願	7	3
外部発表等	研究論文	2	2
	その他研究発表	41	8
	標準化提案・採択	1	1
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	1	0

（7）具体的な実施内容と成果

研究開発項目１： プライバシーを保護する属性ルーティング

1. 属性ルーティング（パナソニック株式会社）

令和元年度に基本部分を設計した、プロデューサ匿名性を Named Data Networking (NDN) 網で提供する匿名ルーティングについて、詳細設計を完了した。さらに、以下の通り、評価ならびにプロトタイプ実装を実施した。第一に、プロデューサ匿名性を厳密に定義し、設計した匿名ルーティングが匿名性を提供できることを検証した。第二に、盗聴だけを行うパッシブな攻撃者と、不正なパケットを送信するアクティブな攻撃者に対する耐性を評価した。この研究成果は IEEE 論文に採択された。さらに、IRTF の ICNRG で匿名ルーティングについて発表し、提案活動を開始した。

一方、実装については、オープンソースの CCN ソフトウェアである Cefore に対して、匿名ルーティングのプロトタイプを実装し、令和元年度に実施した机上検討で計算した性能を達成できることを検証した。また、一部のソフトウェアは GitHub 上に公開した。

2. プライバシ保護ルーティング（大阪大学）

令和元年度に基本部分を設計した、k-匿名性を提供する位置データ検索手法の設計を完了するとともに、シミュレーションにより性能を検証した。具体的には、以下の点について、詳細設計と検証を実施した。第一に、令和元年度に設計した Private Information Retrieval (PIR) を用いた検索手法が、Named Data Networking (NDN) 網で動作できるように、アノニマイザが実行するプロトコルを設計するともに、その安全性を理論的に検証した。第二に、令和元年度に考案した方針に基づいて、アノニマイザがユーザのプライバシーを損なわずに、ユーザがアクセスする目的位置の確率を求める手法を、Local Differential Privacy (LDP) を活用して設計した。さらに、求めた確率から目的位置の k-匿名性を提供する匿名位置集合を生成するアルゴリズムを設計し、中規模の都市で移動する車両を IoT デバイスとして使用する条件でシミュレーションを行い性能評価した。シミュレーションの結果、生成アルゴリズムが、k-匿名性を満たす匿名位置集合を生成できることを検証した。この結果、400 万台規模の IoT デバイスを対象としたプライバシ保護ルーティングが実現できることを検証した。この研究成果について、IEEE 論文に投稿した。

研究開発項目２： 実時間クラウドソーシングアプリケーション

1. アプリケーション設計（パナソニック株式会社）

令和元年度に、多数の移動する IoT デバイスに対して、LPWA (Low Power Wide Area)、セルラー網、インターネットを協調させるシナリオとして、宅配ソリューションにおけるユーザ情報収集の設計と小規模テストベッドによる評価、及び、犯人追跡アルゴリズムの評価とそこで用いる画像データの効率的な収集方法の考案を行った。今年度はそれらを発展させ、宅配ソリューションについては、ICN のオープンソース Cefore を導入し、Panasonic (佐江戸) と大阪大学 (吹田) をインターネットで繋いだ広域テストベッドを完成させた。犯人追跡アルゴリズムについては、シミュレーションにより東京 23 区内の NTT 局舎に LoRa-の GW を設置したモデルでの検証を行うと共に、Cefore を用いた場合の検証も行った。以下にそれらの具体的内容を示す。

宅配ソリューションについては、Cefore 及び LPWA の Cat.M1 を用いた配送トラックからの荷物情報収集機能、LoRa によるユーザへの荷物情報提供機能の各機能について、広域テストベッドへの追加実装を行った。そして、追加実装した機能に関して、効率的な情報収集/情報提供が行えることを検証した。

犯人追跡アルゴリズムのシミュレーション評価については、NTT 局舎のうち、丸の内局舎を RN (Randezvous Node) に見立てた３段階の階層構造を有する情報収集モデルを構築し、LoRa-GW の所要エリアカバー半径の検討を行うと共に、同モデル上で犯人追跡が行えるこ

とを検証した。また、各局舎(ノード)はC++のクラスにて構築しているが、そのうち一部の局舎に Cefore を搭載し、当該局舎間でのデータ受け渡しを Cefore で行うようにしても同様の犯人追跡結果が得られたため、今回構築したモデル上で Cefore が正しく機能していることが確認できた。

なお、以上の取り組みを通じて、国内特許 1 件および外国特許 3 件を出願済である。

2. マルチパス輻輳制御（大阪大学）

令和元年度に基本部分を設計した、Dynamic Adaptive Streaming over HTTP (DASH)を対象とした可変レート動画の輻輳制御方式に対して、詳細設計を完了するともに、シミュレーションによる性能評価を実施した。具体的には、ルータでキャッシュヒットした際に高い符号化レートのセグメントを先読みする手法を、シミュレーションにより評価した。具体的には、複数の符号化レートのセグメントを準備した環境で、先読みアルゴリズムが再生中のセグメントがキャッシュヒットした場合と、そうでない場合の性能を評価した。この結果、セグメントの先読みは平均符号化レートを向上させるが、キュッシュヒットしたかどうかの判定が誤った場合に、平均符号化レートが劣化することを明らかにした。また、令和元年度に設計した遠隔で顔画像認識を実行するアプリケーションに対して、プロトタイプによる性能評価を実施するとともに、オープンソース Cefore へ基本部分を組み込んだ。

（8）研究開発成果の展開・普及等に向けた計画・展望

研究開発成果の展開・普及に向けて以下の通り取り組む予定である。第一に、実用化に対しては、匿名ルーティング技術のオープンソース化を進める。オープンソース化については、NICT が開発中の ICN のオープンソース Cefore に組み込み、開発したソースコードを公開する。既に、基本部分のソースコードは、Cefore に組み込み、GitHub に公開しており、研究開発終了後は、匿名ルーティングのソースコード全体を公開する。第二に、標準化に対しては、ICN の標準化を行っている IRTF の ICNRG において、プロデューサ匿名ルーティングの標準化活動を進める。

第三に、広報活動については、まず、学術的には成果を一流の国際論文誌に投稿するとともに、一流のマガジンに投稿する。現在、IEEE と Elsevier の論文誌に投稿中である。次に、一般向けには、Web での広報を行う。現在、大阪大学の研究室のホームページで研究成果を公開中であるが、デモビデオ、研究開発終了後の活動についても、公開を続ける。

第四に、製品化等、成果の産業応用については、特に今後「現場プロセス」として力を入れる領域の一つである流通への応用を想定している。また、ICN についてはスマートシティ間で IoT データの相互利用を行うためのプラットフォームに適用することも検討する。

今後の展望については、研究開発を開始した当初と比較して、巨大 IT 企業の市場独占に伴う、プライバシー漏洩に対する懸念が高まっており、研究開発成果のプライバシー保護技術を利用する場面が多くなると期待される。例えば、新型コロナウィルス対策のため、接触した人を Bluetooth で検知し、接触履歴を管理するアプリケーションが、プライバシーに対する懸念などで普及したなかったのに対して、プライバシー保護技術はこのようなアプリケーションの普及に貢献することが期待される。さらに、今後はユーザが提供する教師データを用いた機械学習サービスの普及が予想されており、プライバシー保護技術は安心で安全なサービスの提供に貢献することも期待される。