様式１－４－２

平成 29 年度研究開発成果概要書

採 択 番 号 ：19101
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年度から平成３２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（平成２９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

1. 属性ルーティング（パナソニック）

位置を取り上げ、屋外から屋内で必要な精度で位置を測定する技術をベースに、任意の変更可能な精度で指定した位置のエリアに存在する IoT デバイス群に、センサデータを要求するパケットを転送するルーティング方式を設計する。位置の指定には ICN(Information Centric Networking)を用いることを想定し、Z 座標などの一次元で、かつ位置の精度を制御可能な手法を開発することにより、400 万台規模の IoT デバイスの位置を示す経路情報を集約する。さらに、位置以外の属性を用いたより細やかなセンサデータ情報を指定できるように拡張する。

2. プライバシー保護ルーティング（大阪大学）

センサデータに含まれる秘匿情報を、事前の公開鍵配布などの複雑な鍵交換処理を行うことなく、アクセス権限を与えた収取者だけが復号可能とするように、マルチキャストと ABE を組み合わせたセンサデータの収集方式を開発する。さらに、提供者の IoT デバイスの位置や、収集者がアクセスした位置に関して漏れるプライバシーの量を表現する匿名性の指標を考案し、漏れるプライバシーの量と、プライバシー保護に必要な通信オーバヘッドのトレードオフを調整可能な収集方式を、匿名ルーティング、あるいは秘密分散を属性ルーティングに組み合わせることで実現する。

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）

収集者があらかじめ指定したトピックと位置に合致するIoTデバイスが取得したセンサデータを、アクセスを許可された収集者だけに自動的に配信するクラウドソーシングアプリケーションを開発する。ここで、トピックや位置は属性ルーティングの属性として扱う。スタジアムにおいて、他の観客が撮影した収集者が見えないアングルでの映像を自動的に収集するアプリケーションや、事故や犯罪が起こった際に、容疑者を追尾して、街中やビル内に異なる管理者が設置したカメラが撮影した映像を収集するアプリケーションを例として、設計する。さらに、ICNテストベッドを用いて、開発したアプリケーションを評価する。

2. マルチパス輻輳制御（大阪大学）

IoT デバイス群から大量データが同時刻に発生するため、ネットワーク上のとりわけエッジに近い領域における輻輳制御が重要な課題である。これに対して、複数無線アクセスネットワークから構成される5Gネットワークを対象として、ルータの持つキャッシュを用いたネットワーク主導のマルチパス輻輳制御を開発する。具体的には、個々のルータが、機械学習により複数のパスを利用して輻輳を回避しつつ、機械学習の概念に脳や生体が局所的な性能のフィードバックにより生体ゆらぎを制御する手法を応用することで、ネットワークの状態を安定化させつつ、準最適なパスの選択を可能にするアルゴリズムを開発する。

（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	7	6
	外国出願	1	1
外部発表	研究論文	0	0
	その他研究発表	15	9
	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１： プライバシーを保護する属性ルーティン

1. 属性ルーティング（パナソニック）

宛先の位置をZ-記法で表記する名前機構を設計し、NDN網上でのパケット転送用のデータ構造(Subscription Table: ST と呼ぶ)と、位置のプレフィクス検索条件とフォワーディングアルゴリズムを開発した。トライ木とZ-記法の4進数の特性を考慮した圧縮により、第一の中間目標の400万台規模の経路情報の集約に対して、PC ベースのルータに実装可能なほど集約できることを、シミュレーションにより明らかにした。さらに、第二の中間目標である属性の拡張について、IoT デバイスがデータ種別を指定できるように名前機構を拡張し、フォワーディングアルゴリズムと階層的トライ木を用いたデータ構造を開発した。

2. プライバシー保護ルーティング（大阪大学）

属性ベース暗号とマルチキャストを組み合わせて、指定する属性を第三者から秘匿するプライバシー保護ルーティングの設計を完了する。第一の目標である、マルチキャストの範囲に対する転送データ量とk-匿名性のトレードオフ関係は、シミュレーションにより明らかにした。さらに、位置情報が漏れないためのマルチキャストの範囲に関する条件を明らかにするとともに、匿名性の指標として、k-匿名性にl-多様性を組み合わせた指標を設計し、その安全性を検証した。第二の目標である、複雑な鍵管理を必要とし

ない認証方式については、データを要求するIoTデバイスの位置をABEの属性の公開鍵に対応させることで実現した。

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）

位置属性を用いる様々なユースケースを検討し、その中から特に複数の属性を用いたケースを抽出した。抽出したケースの一つは、位置情報と街中の防犯カメラのよる画像検出を用いて逃走犯の追跡を行うもので、シミュレーションによって追跡アルゴリズムの評価を行った。もう一つのケースは、位置情報と温度情報から火事の有無を検出するもので、小規模な実証実験装置を構築し、COPSS方式によるルーティング、NFDによるデータ転送、およびABEによる暗号化を搭載し、火事の判定がリアルタイムにできること(複数属性による判定ができたこと)、火事と判定された位置の動画像をダウンロードして表示できること(判定結果によって異なるアクションができること)、更にはその動画像が許諾された収集者にしか見ることができないこと(ABEが正しく動作していること)を検証した。

2. マルチパス輻輳制御（大阪大学）

IoTデバイスから収集する情報によるエッジネットワークの輻輳を解消することを目的としたマルチパス輻輳制御として、否定応答を用いた輻輳通知と各ルータが保持するパケット転送情報を用いたホップバイホップの輻輳制御を設計した。具体的には、各ルータにおいてFIBのエントリ単位およびフェイス単位で輻輳状況を計測する。輻輳を検出したルータは、上流ネットワークに否定応答を送信する。否定応答を受信したルータは、計測していた、FIBエントリ単位およびフェイス単位輻輳状況を調整し、その情報に基づいてインタレストの転送レートを制御する。このフォワーディング方式についてシミュレーションにより評価し、レート制御によりネットワークエッジに流入するインタレストパケット量を適切に制御でき、ネットワークエッジにおける輻輳を解消できることを示した。