様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２５　日現在

機関番号：　８２６３６
研究種目：　若手研究(B)
研究期間：　2016～2017
課題番号：　１６Ｋ１６０５４

研究課題名（和文）Secure and Efficient Data Sharing for Information-Centric IoT

研究課題名（英文）Secure and Efficient Data Sharing for Information-Centric IoT

研究代表者
李　睿棟（Li, Ruidong）

国立研究開発法人情報通信研究機構・ネットワークシステム研究所ネットワーク基盤研究室・研究員

研究者番号：４０５３６０８３

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：　従来のネットワークシステムは、主にクラウドをベースとしたエンドツーエンドでモノのインタネット（IoT)サービスを提供している。そのため、重複データ転送や遅延増加などの欠点が存在する。IoT時代では、センサーデータのネットワーク内キャシングが発展するにつれて、効率的且つセキュアセンサーデータ流通への需要も高まってくる。
　この需要を満たすため、センサーデータがネットワーク内に遍在的にキャシングされるシナリオにおいて、情報セントリックネットワーキング技術を用い、低遅延且つ低コストの多対多データ流通および分散的センサーデータのセキュア取得を提供できる新しい機構の研究を行った。

研究成果の概要（英文）：　The existing network systems mainly provide Internet of Things (IoT) service through cloud-based end-to-end communications, which leads to the disadvantages, such as duplicate data transmission and increased delay. In the IoT era, with the development of the in-network caching of sensor data, the demand for efficient and secure sensor data distribution greatly increases.
　To satisfy this demand, we utilize the information-centric networking (ICN) technology to investigate two issues: 1. Design and evaluate the efficient sensor data collection and publication protocols for IoT scenarios using ICN approach. 2. Design and evaluate a secure and flexible sensor data retrieval mechanism to establish trust between the distributedly cached sensor data and users.

研究分野：　情報学

キーワード：　もののインターネット　情報セントリックネットワーキング　多対多通信　セキュリティ　アクセスコントロール

１．研究開始当初の背景

モノのインターネット（IoT）は、数十億のものがつながり、膨大な量のデータが共有されるインターネットの次の進化の主要なトレンドの1つとして浮上している。IoTは、ヘルスケア・スマートシティ・公共安全・スマートグリッド・交通・農業など、さまざまな分野で大きな可能性を秘めたシナリオを用意している。 IoT が採用されている場合、IoT データの基本的な共有手順は、センサおよびアクチュエータからデータを収集し、ユーザグループにデータを共有し、その後に 1 つまたは複数のストレージポイントからデータを取得することになる。ヘルスケアの例として、健康状態を測定し、医師に報告するために、血圧および温度センサからデータを要求される。その後、このデータを他の医師・家族・時には近隣の人に共有し、いくつかの記憶ポイントにキャッシングまたは格納する。関係者はこれらのストレージポイントからデータを安全に取得する必要がある。

これらの手順には、いくつかの課題がある。第１に、クエリブロードキャストは主にセンサからデータを収集するために使用され、非効率的である。フラッディングオーバヘッドとクエリ時間を抑えるために、クエリを自動的にターゲットセンサに誘導し、関連のデータを順番に収集する技術が必要である。第 2 に、ユーザグループにデータ共有を実現するデータセンター技術は、ユーザ達に重複したデータ送信のために、多くのトラフィックオーバーヘッドをもたらす。同様に、P2P 技術が使用される場合、多くのトラフィックオーバーヘッドは、データ伝送とインフラストラクチャとの間の不一致のために引き起こされる。第 3 に、センサデータは、いくつかのまたは多数の記憶域またはキャッシポイントに分散してキャッシングされる。移動性やネットワーク状態のため、データを取得するストレージポイントを頻繁に変更することがある。データがネットワークに分散してキャシングされるため、センサデータとユーザ間の相互信頼は確立されにくい。対照的に、現在のアドオンセキュリティメカニズムは、ホスト中心の通信モデルに基づいて設計されており、データが分散キャッシュされている場合、認証可能なデータ取得問題をうまく解決できない。

これまで、エンド・ツー・エンド通信に基づいて、小型デバイスを IoT でインターネットに接続する方法に関する膨大な数の研究が行われている。しかし、IoT は当然情報中心であり、ユーザーはデータがどこから収得され、キャッシュされているかにかかわらず、データ自体のみを気にする。したがって、エンドツーエンド設計は、複雑なコンフィグレーションとセンサノードでのエネルギー消費をもたらし、一方、グループ内でデータを共有するときには不要な通信オーバーヘッドを引き出す。また、予測できないキャッシングやセンサデータの格納場所からの安全なデータ取得にも課題がある。

一方、情報中心型ネットワーキング（ICN）は、場所に関係なく名前を使用してデータを取得することを提唱する新しいコミュニケーションのパラダイムとして浮上している。また、データ取得を容易にするために、ネットワーク内のキャッシュを使用する。従って、IoT のための通信を提供する有望な候補者となっており、これはここでは「情報中心 IoT」と呼ばれている。 CCN、PURSUIT、NetInf などの既存の ICN ネットワークは、名前ベースのデータ検索の基本機能を実現した。しかし、それらのどれも IoT サービスを可能にするために主に設計されたものではなく、これらの課題はまだ未解決の問題として残っている。

２．研究の目的

従来のネットワークシステムは、主にクラウドをベースとしたエンドツーエンドで IoT サービスを提供している。そのため、重複データ転送や遅延増加やセキュリティ脆弱性などの欠点が存在する。IoT 時代では、センサデータのネットワーク内キャシングが発展するにつれて、効率的且つセキュアセンサデータ流通への需要も高まってくる。

この需要を満たすため、センサデータがネットワーク内に遍在的にキャシングされるシナリオにおいて、情報セントリックネットワーキング技術を用い、低遅延且つ低コストの多対多データ流通および分散的センサデータのセキュア取得を提供できる新しい機構の研究を目的とする。

３．研究の方法

我々は、上記の目的を目指し、ほぼ空白の研究領域である情報中心 IoT のための安全で効率的なセンサデータ共有の枠組みを設計する。下記の二つの課題を分けて年度計画をセッティングし、計画の通り研究を遂行した。

課題１：情報中心 IoT の効率的なセンサデータ共有プロトコルを設計する。

課題２：安全で柔軟なセンサデータ取得機構を設計する。

この二つの課題を巡って、具体的に下記計画の様に研究を行った。

	28 年度	29 年度
課題１	ICN ベース多対多通信研究調査・アルゴリズム設計	性能分析・成果発表
	研究協力者：朝枝仁、Klaus Moessner	

課題２	ICN ベースデータ取得アクセスコントロールに関する研究調査とアルゴリズム設計・性能分析・成果発表	ICN ベースデータ取得認証・トラストに関する研究調査とアルゴリズム設計・性能分析・成果発表
	研究協力者：朝枝仁、Jie Li，Xiaoming Fu	
結合	低遅延且つ低コストの多対多データ流通および分散的センサデータのセキュア取得仕組みの設計	

具体的な研究方法は下記の様である。

課題１：情報中心 IoT の効率的なセンサデータ共有に関しては主に２つの効率的な問題がある。１つは頻繁なクエリフラッディングで、１つのクエリでもセンサに多くのトラフィックオーバーヘッドとエネルギー消費をもたらす。もう１つは、１つのデータが１つのクエリによって取得され、多数のクエリ回数につながることである。これらの問題を解決するために、センサデータの命名設計と多対多ルーティングアルゴリズムを設計する。更に、性能に影響する重要な要因を調査し、効率的な通信のための決定アルゴリズムとスイッチングメカニズムを設計する。

課題２：安全で柔軟なセンサデータ取得機構を設計する。分散的にキャッシュされたセンサデータへの安全なアクセスのために、分散型認証およびデータアクセスコントロールを効率的に提供するのは困難である。これらの問題を解決するために、我々は属性ベースの暗号を利用し、分散アクセス制御を行えるようにする。更に、センサデータ所有者、ネットワークプロバイダ、ユーザ、およびキャッシュ可能ルータ間のセキュリティ関係を特定し、信頼関係を構築方法を設計する。

４．研究成果

課題１と２を分けて具体的に下記の様な研究成果に達成できた。

課題１：情報セントリックネットワーキング技術を利用し、効率的な多対多データ取得と転送の実現可能性を調べ、新たな多対多通信アルゴリズムを設計し、ルートデバイスの置き場所と数から多対多通信性能への影響を調べた上で、計算量の少ない最適化されたルート選択アルゴリズムを提案した。シミュレーションで性能評価を行い、提案アルゴリズムにより、トラフィックを低減できることを示した。[5.学会発表④参照]

課題２：センサデータをネットワーク内で遍在的にキャシングを行う IoT 環境では、データの分散アクセス制御が大変困難になる。この問題を解決するため、これまでの認証と暗号技術を調査しつつ、分散的データ取得に対する脅威分析を行い、CP-ABE を用い、分散的にキャシングされた IoT データを許可されたユーザのみが収得できるようにする新しい分散型パブリッシャー駆動セキュアデータ共有スキーム (DPD-ICIoT) を提案した。DPD-ICIoT では、属性マニフェストが新規に導入されるとともに、ネットワークにキャシングされ、パブリッシャーは集中的な属性サーバではなく近くにあるデバイスから属性値を取得できるようになる。更に、効率的な暗号操作のためにキーチェーン機構が利用されており、属性値自動更新メカニズムを提案することにより、集中サーバに問い合わせることなく属性の高速更新も可能にする。モデリング技術にて、提案したスキームにより、バンド幅の利用量を低減できることを検証した。[5.雑誌論文②と学会発表③参照]

ネットワーク内データへのアクセスコントロールアルゴリズムの設計と検証の上で、身分確認に対する脅威分析に基づきセキュリティ要件を明確化した。そして、ID ベース暗号を用い、ネットワーク内データ取得を保護できる分散的認証・認可スキームを提案した。モデリング技術にて、提案した分散的認証・認可スキームにより、バンド幅の利用量を削減できることを検証した。[5.雑誌論文①と学会発表②参照]

更に、任意のエンティティから別のエンティティに認証できるように、サスペンションチェーン（SCM）というトラストモデルを設計し、新しいデータ中心型 any-to-any 認証方式である DataTrust を提案した。また、提案方式の DataTrust のコストを評価するためにシミュレーションを実行した。[5.学会発表①参照]

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　2　件）

① Ruidong Li、Hitoshi Asaeda、Jie Li、Xiaoming Fu 、“A Distributed Authentication and Authorization Scheme for In-Network Big Data Sharing”、 Elsevier Journal of Digital Communications and Networks、査読有、 vol.3、 issue 4、2017、226-235 DOI: 10.1016/j.dcan.2017.06.001

② Ruidong Li、 Hitoshi Asaeda、 Jie Li、“A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT”、 IEEE

Internet of Things、査読有、vol.4、issue 3、2017、791-803
DOI: 10.1109/JIOT.2017.2666799

〔学会発表〕(計 4 件)

① Ruidong Li、Hitoshi Asaeda、"DataTrust: A Data-Centric Any-to-Any Authentication Scheme"、査読無、IEICE IA Technical Report、Mar. 5、2018.日本・日光

② Ruidong Li、Hitoshi Asaeda、Jie Li、Xiaoming Fu、"A Verifiable and Flexible Data Sharing Mechanism for Information-Centric IoT"、査読有、IEEE International Conference on Communications (ICC 2017)、May 2017.フランス・パリ

③ Ruidong Li、Hitoshi Asaeda、"DPD-ICIoT: A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT"、査読無、IEICE IA Technical Report、A2016-85、Jan. 27、2017.日本・東京

④ Ruidong Li、Hitoshi Asaeda、Klaus Moessner、"Optimized Root Selection Algorithm for Many-to-Many Communications in ICN"、査読有、The 11th International Conference on Future Internet Technologies (CFI 2016), June 15-17 2016.中国・南京

６．研究組織

(1)研究代表者

李 睿棟 (LI, Ruidong)
国立研究開発法人 情報通信研究機構・ネットワークシステム研究所 ネットワーク基盤研究室・研究員
研究者番号：４０５３６０８３

(2)研究協力者

- 朝枝 仁 (ASAEDA Hitoshi)
  国立研究開発法人 情報通信研究機構・ネットワークシステム研究所 ネットワーク基盤研究室・研究マネジャー
- Klaus Moessner (MOESSNER Klaus)
  イギリス・University of Surrey・Department of Electrical and Electronic Engineering・教授
- Jie Li (LI Jie)
  筑波大学・コンピュータサイエンス専攻・教授
- Xiaoming Fu (FU Xiaoming)
  ドイツ・University of Gottingen・Institute of Computer Science・教授