（革新）様式 1-4-2 (2021-2)

令和３年度研究開発成果概要書

採 択 番 号　　03901
研究開発課題名　超多数・多種移動体による人流・物流のためのダイナミックセキュアネットワークの研究

（１）研究開発の目的

官民 ITS 構想・ロードマップや空の産業革命に向けたロードマップ 2021 に掲げられている目標達成に必要な、移動体を高密度、超多数で安全に協調稼働させるセキュリティ基盤技術の開発である。

具体的には、アグリゲートメッセージ認証等によるセキュアかつ高効率な認証、高信頼な位置情報の取得方式、及び分散台帳による高信頼で柔軟な情報秘匿・共有等の技術から構成されるセキュリティ基盤技術を開発する。

本研究では、「開発技術候補例リスト」(5-3) に書かれている、セキュアで広域の高信頼性、超低遅延通信（URLLC）を実現し、現在の 5G 通信を超える、超高速、大容量、超低遅延、超多数同時接続の機能を活かしたセキュリティ基盤技術を目標とする。

（２）研究開発期間

令和３年度から令和５年度（３年間）

（３）受託者

ジャパンデータコム株式会社（JDC）＜代表研究者＞
学校法人早稲田大学（早稲田大学）

（４）研究開発予算（契約額）

令和３年度から令和４年度までの総額 100 百万円（令和３年度 17 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　ワイヤレス通信の効率的かつセキュアな情報交換のための要素技術研究
1-a) 通信効率性の高い認証方法（JDC）
1-b) 柔軟性が高く検証可能な属性提示方法（早稲田大学）
1-c) 信頼性の高い位置情報の生成・記録（早稲田大学）
研究開発項目２　ソフトウェア・ハードウェア実装に向けた応用研究（JDC）

（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	1	1
	外国出願	0	0
外部発表等	研究論文	0	0
	その他研究発表	1	1
	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	0	0

（7）具体的な実施内容と成果

本研究では、次の二つのシナリオを想定し、各項目の研究開発を実施している。

①「移動体の衝突防止のためのシナリオ」

（多数のドローンが衝突せずに空中交通レーン飛行が可能）

研究開発項目：

1-c)各ドローンの信頼性の高い位置情報の生成・記録

1-a)通信効率性の高い認証方法による位置情報のドローン間の共有

2)提案方式の確認・評価が可能なセキュリティ基盤（プロトタイプ）の実装

②「物資管理のためのシナリオ」

（多数のドローン搭載物資の確実な認証・追尾、物資・送受者情報の保護が可能）

研究開発項目：

1-b)搭載物資に関する柔軟性が高く検証可能な属性提示

1-a)通信効率性の高い認証方法による管制センタでの搭載物資の認証・追尾

2) 提案方式の確認・評価が可能なセキュリティ基盤（プロトタイプ）の実装

研究開発項目１：ワイヤレス通信の効率的かつセキュアな情報交換のための要素技術研究

1-a）通信効率の高い認証方法

通信効率の高い認証方法として、アグリゲートメッセージ認証による相手認証技術とデジタル署名に基づくアグリゲート署名技術について研究開発を進めている。

アグリゲートメッセージ認証による相手認証技術では、本研究が想定するシナリオ下における、完全性が求められる情報の収集及びメッセージ認証子の集約、及び検証を自動化して行うような相手認証技術について開発するために、令和３年度には、シナリオ上で想定される課題に対して検討した。その結果、検証サーバと移動体との通信を中継するサーバの間で対話的処理を行えば中継サーバがカバーするエリア内すべての移動体の相手認証に必要なデータ量を従来技術に比べて削減可能であるという知見を得た。

デジタル署名に基づくアグリゲート署名技術では、本研究が想定するシナリオ下における、完全性が求められる情報の収集・集約を行う際、秘密鍵・公開鍵を用いたデジタル署名による、アグリゲート署名技術の検討を行った。既存技術としてペアリングに基づく構成、格子構造に基づく構成が知られているが、令和３年度はその拡張性に関して検討し、その結果、格子構造に基づく構成の拡張として、署名集約アルゴリズムと検証アルゴリズムの間にグループテストアルゴリズムを応用することにより、不正メッセージを特定する構成が可能という知見を得た。

1-b）柔軟性が高く検証可能な属性提示方法

多種多様な移動体が柔軟性高く、その正当性について検証可能な形で属性開示する方法の実現にむけて、基礎的なシナリオでの検討を行うための調査・初期設計を行った。具体的には、まず、ISO で定められたグローバルな ID 体系である取引主体識別子（LEI）とそれを VC 化した vLEI について調査した。二人の所有者がそれぞれ２台の移動体所有を想定し、所有者はそれぞれ２台の移動体に VC を発行し、どの４台の移動体も、第三者に自身の所有者の情報を検証可能な形で提供できる手法を設計した。その結果、本研究が想定するシナリオに適用可能である知見を得た。また、所有者情報を第三者に提供した際、第三者が記録する検証ログから、所有者を確認できても、移動体自身は特定できないが、その検証ログを所有者に還元した場合は、所有者は提供した移動体が特定できる方式の調査・検討を行った。なお、調査した vLEI は、所有者の認証に用いることを想定しており、今後検討を行う。

1-c）信頼性の高い位置情報の生成・記録

信頼性の高い位置情報の生成・記録の研究では、GNSS、Bluetooth ビーコン、Wi-Fi、画像、その他の測位技術などの複数の位置収集手段による統合処理などを用いて信頼・信用できる位置情報を獲得し、近接する実空間移動体へ伝達する情報を生成する技術について、方式の調査・試作・評価を行った。位置情報の生成については、種々の外乱・妨害に対して、GNSS と Wi-

Fi またはアクセスポイントから得られる位置情報を合わせて検証する手法を検討した。簡単な実験において、位置情報の偽装を98%以上検出できる知見を得た。事故等の検証用の位置情報の記録方法については、本研究が想定するシナリオにおいて改ざん発生ゼロとなる方法について調査比較を行い、検証する構成案を複数抽出した。

研究開発項目２：ソフトウェア・ハードウェア実装に向けた応用研究

令和３年度は、貨物配送ドローンやドローンカーなどのエアモビリティ、自動運転車などの移動体が超多数・超多種存在し、異なる運営会社の間で混在運用される配送システムにおけるセキュリティ基盤（プロトタイプ）の実装・評価に向けて、本研究で想定するシナリオに合致する無線通信方式の選定のため、ローカル5G、Wi-Fiなどの考えうる通信手段について複数の機器ベンダーのヒアリングを含め調査し、通信仕様等の知見を得た。また、ドローン物流サービスプラットフォーム事業者とのヒアリングを含めドローン物流の現状を調査し、ドローン物流の現状・課題についても知見を得た。

上記調査成果を踏まえ、「移動体の衝突防止のためのシナリオ」については首都高上空に設置された空中交通レーンを飛行する大量のドローンの交通制御を行うシナリオ、「物資管理のためのシナリオ」については車両とドローンを併用し、複数の発送先へ大量の物資を配送するシナリオとし、①「衝突防止シナリオに関する実験」および②「物資管理シナリオに関する実験」の為に令和４年度に構築するプロトタイプの仕様（原案）および、③「超多数・超多種接続に関する実験」の為に令和４年度に実施するソフトウェアシミュレーションの仕様（原案）を作成した。

（８）今後の研究開発計画

研究開発項目１：ワイヤレス通信の効率的かつセキュアな情報交換のための要素技術研究

1-a）通信効率の高い認証方法

アグリゲートメッセージ認証技術による相手認証技術では、令和３年度に検討した研究内容に基づいて、検証サーバと移動体との通信を中継する中継サーバの間で対話的処理を行うことにより中継サーバがカバーするエリア内すべての端末の相手認証に必要なデータ量を従来技術に比べて削減する方式を完成させる。

デジタル署名に基づくアグリゲート署名技術では、令和３年度に検討した拡張性に関する研究を進め、本課題が想定するシナリオ下における効果的な情報の収集・集約を実現する方式を検討する。

1-b）柔軟性が高く検証可能な属性提示方法

令和３年度に検討した属性提示方法について試作を行い、機能検証を行う。令和３年度に基礎検討した基盤を元に、グループ署名の特徴である、問題があった場合に、平常時に開示していなかった移動体を特定する情報を、ログを活用して検証可能な方法で提供できる枠組みを追加する。

1-c）信頼性の高い位置情報の生成・記録

令和３年度に検討した位置情報の偽装検出方法については、さらに位置情報の信頼性を高める他の手法も加え、試作・評価をおこなう。複数の位置計測手段から得られるデータとアクセスポイントの特性、さらに位置計測データの時系列の履歴を用いて「信頼度」を求めるアルゴリズムを開発する。位置情報の検証の処理時間は0.04秒以内に収まることを確認する。さらに、事故等の検証用に求められる移動体の位置情報の記録についても、令和３年度に抽出した手法に対する試作・評価を行い、シナリオに対してリスク事象が発生しないことを確認する。

研究開発項目２：ソフトウェア・ハードウェア実装に向けた応用研究

本研究が想定するシナリオについて、研究開発項目１の要素技術の研究開発成果の評価を可能とするセキュリティ基盤（プロトタイプ）を開発し、以下の三つの実験・評価を行う。

①「移動体の衝突防止のためのシナリオ」に関する実験

ドローンなどの移動体の自律制御に際し、研究開発項目 1-c により得られる信頼性の高い位置情報を、研究開発項目 1-a のアグリゲートメッセージ認証、あるいはアグリゲート署名を用いて位置情報を中継するサーバで集約（アグリゲート）するあるいは各々の移動体で集約する場合について、令和 4 年度は移動体の機能を模擬するデバイス、中継サーバの機能を模擬するサーバで構成される小規模なプロトタイプを構築して実験・評価を行い、研究開発項目 1 の提案方式を実証する。

②「物資管理のためのシナリオ」に関する実験

貨物ドローンなどの移動体を用いた大量の物資を管理しながらの流通に際し、研究開発項目 1-b にて検討される柔軟性が高く検証可能な属性提示方法と研究開発項目 1-a のアグリゲートメッセージ認証を組み合わせ、物資に付与されたスマートタグの情報を、完全性を担保しながら集約し、検証するための方式について、令和 4 年度は移動体の機能を模擬するデバイス、中継サーバの機能を模擬するサーバで構成される小規模なプロトタイプを構築して実験・評価を行い、研究開発項目 1 の提案方式を実証する。

③「シナリオ①②における超多数・超多種接続」に関する実験

簡易的なソフトウェアプロトタイプを構築し、超多数・超多種接続を考慮した実験を行う。本実験・評価により、超多数・超多種接続時においてもシナリオ①の中間目標である片道処理時間が 0.04 秒、往復応答 0.1 秒未満、シナリオ①②の中間目標である 66%以上の周波数帯域削減効果を達成できる見込みであることを確認する。

また、実装するソフトウェアプロトタイプ（シミュレーション環境）とハードウェアプロトタイプを実証評価するために、有効性、機能性、性能などの評価項目の抽出と評価方法の検討を行い、具体的な利用シーンを考慮して評価を実施する。令和 4 年度も引き続き、ドローン制御プラットフォーム開発会社などへのヒアリングを行い、それを基に整理された配送システムに必要とされる要件、評価項目を確立させる。