（革新）様式 1-4-2 (2022-1)

令和４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４年度 83 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	2	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	9	8
	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

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）

アグリゲートメッセージ認証技術による相手認証技術の研究では、アグリゲート相手認証（片側認証方式）における形式的モデル、セキュリティ要件の定式化を行い、グループテストとメッセージ認証（MAC）による一般的構成法を開発した。本成果は査読付きの国際会議（2023 IEEE Information Theory Workshop）に採録されたため、今後、当該会議にて論文発表する。また、本開発技術のソフトウェア実装評価を行って実用性を示し、その成果を国際論文誌に投稿した。さらに、これら成果を拡張し、アグリゲート相手認証（相互認証方式）、メッセージ認証とエンティティ認証を同時に行うことが可能なアグリゲート認証方式の構築も検討した。

アグリゲート署名技術の研究では、アグリゲート署名技術に関わる既存研究の調査解析を行った。また、既存の格子ベース構成のアグリゲート署名において、集約者と検証者（サーバ）の間でグループテストアルゴリズムを実行することにより、不正データを特性することが可能となる方式を検討した。さらに、デジタル署名ベースのアグリゲート相手認証方式（片側認証方式）の構築の基礎検討を行った。これら成果については、今後、完成度を高めて学術論文として公表する予定である。

1－b）柔軟性が高く検証可能な属性提示方法（早稲田大学）

W3C における DID と VC 方式によるフレームワークを調査し、このフレームワーク上に VP を活用することでグループ署名を可能とする基盤を構築・試作し、課題を抽出した。

また、柔軟性高く検証可能な属性提示方法を実現する物資管理シナリオを想定したプロトコルを策定した。同プロトコルについて、二人の所有者がそれぞれ２台の移動体を所有するという基礎的なシナリオを想定し、開発手法の妥当性を確認した。また、所有者情報を提供したどのログから提供した移動体が特定できることを確認した。

1－c）信頼性の高い位置情報の生成・記録（早稲田大学）

信頼性の高い位置情報の生成については、精度の高い偽装検知方法として時系列データの機械学習に適した LSTM ネットワークを適用し、ソフトウェアを試作、機能および性能の検証を実施し、高い適合率 0.97 と再現率 0.93 の両立など性能改良を確認した。偽装検知の処理時間は、0.7 ミリ秒以下で、位置情報の交換の目標時間 0.1 秒に対して十分小さいことを確認した。

信頼性の高い位置情報の記録については、各種手法の調査に基づき、研究開発項目 1-a)のメッセージ認証に準ずる形で記録する方法に対してリスク分析を行い、想定するユースケースレベルでの問題発生をゼロとする時系列データの記録方法を試作、機能確認を行った。

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（JDC）

想定される２つのシナリオについて、プロトタイプシステムを用いた実験・評価を進め、想定した性能の見通し、および想定したセキュリティリスクへの対応を確認した。衝突防止のためのプロトタイプシステムでは、１編隊が 10 台の場合（構成Ａ）と各編隊 5 台の 2 編隊構成（構成Ｂ）での評価を行い、応答時間の実測値は目標値を上回ったものの、今後の同期処理の最適化やハードウェア性能の向上によっていずれの場合でも目標値を達成する見込みであることを確認した。また、物資管理シナリオのプロトタイプシステムでは、搬送する物資リストが 1000 個あるとき、複数の仕分けパターンにおいて実装評価を行い、メッセージ認証子異常の検知可能数が最大 4 までの場合において 66%以上の周波数帯域削減効果の目標値を達成する見込みであることを確認した。物資管理シナリオのプロトタイプには課題 1-b の VC 方式を活用したプロトコルも組み込み、互いに干渉なく動作することが確認できた。

（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）通信効率性の高い認証方法（JDC）

アグリゲートメッセージ認証による相手認証技術では、研究開発項目２で実施する100 万台以上のスマートタグ情報を管理することを想定したシミュレーションによる性能評価結果を分析し、66%以上の周波数帯域削減効果を得ることを確認し、また共通鍵等の管理用方式を考案・整理する。

アグリゲート署名による相手認証技術では、前年度に構築した基本方式の分析・評価により更なる改良・拡張等を目指す。

1－b）柔軟性が高く検証可能な属性提示方法（早稲田大学）

それぞれの組織が所有するドローンや自動運転車などの移動体を一つ一つ識別する属性について、同じ属性を持っている相手に対して、鍵共有による暗号通信が可能になる機能を提供する。

また、概念実証（PoC）により、各組織において新規移動体の追加を容易にし、想定したシナリオに対して、偽造された属性や、古い属性を提供した場合に、提示先が正しくそのことを見破ることができることを確認する。同様に、想定したシナリオに対して、制御ミス、記録ミス、監査不能の発生がないことを確認する。

1－c）信頼性の高い位置情報の生成・記録（早稲田大学）

信頼性の高い位置情報を生成するための検証処理について、片道処理時間が 0.04 秒、往復応答 0.1 秒以内に完了することを確認する。また、PoC や実証実験において、設定したユースケース・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（JDC）

研究開発項目１の成果を組み込んだプロトタイプでの性能評価による小規模なモデルでの性能評価を実施、目標性能の実現可能性を示すことができた前年度の成果をベースに、大規模環境を想定したシミュレーションにより性能評価を行い、大規模環境下での目標性能の実現可能性を確認する。衝突防止シナリオについては、ドローンの位置情報送信から飛行制御情報入手までの遅延時間が 0.1 秒の実現可能性とその場合の要件等を整理する。物資管理シナリオについては、100 万台以上のスマートタグ情報の送信における付加するセキュリティ情報の 66%以上の周波数帯域削減効果を得ることを確認し、そのための要件等を整理する。

また、小規模環境での機能・性能評価のために前年度に構築した衝突防止シナリオに関するプロトタイプをベースに、デモシステムを構築、イベント等でのデモによる社会認知・普及活動を展開する。