（革新）様式 1-4-2 (2022-1)

令和５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

Beyond5G/6G の時代には地上は自動運転車などが、空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が時空間的に密に行き交い、ヒト・モノ・コト流を支えるような超多数・多種な移動体の密な空間での協調稼働による、時空間の有効利用が期待されている。これらの移動体は複数の運営会社によって管理・運営されており、お互いに交信しながら運航しており、従来の地上の交通網に比べて高速で快適な人流・物流・サービス流が提供できるようになると想定している。

実空間上を移動し人や重量物を運搬するため、それらの３次元的なナビゲーションは、応答速度の速さのみならず、きわめて信頼性の高いものが求められ、自然現象による GPS 信号への外乱や鳥・妨害ドローンなどからの障害に耐える必要がある。また、フィジカル空間上を行きかう移動体の位置情報、LIDAR 情報などのセンシング情報や貨物に含まれるスマートタグの情報は同一グループ内・異グループ間など情報伝送・交換する範囲の柔軟性が確保されたうえでのセキュアな通信も求められる。また、セキュリティを確保するためにはメッセージ認証子などのオーバーヘッドを情報に付与する必要性があるが、その情報を伝達するための周波数帯域も依然重要なリソースであり、より効率よく伝送しなければならい。

本研究開発では、通信効率性の高い認証方法、柔軟性が高く検証可能な属性提示方法および信頼性の高い位置情報の生成・記録方式を確立することで、超多数・多種移動体が安全に協調した物流に不可欠なセキュリティ基盤技術を開発し、その結果として従来技術ではひっ迫される無線リソースを軽減することを目標にする。

（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＜代表研究者＞
学校法人早稲田大学

（４）研究開発予算（契約額）

令和３年度から令和５年度までの総額 130 百万円（令和５年度 30 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方法のための要素技術研究
研究開発項目１-a)通信効率性の高い認証方法（ジャパンデータコム株式会社）
研究開発項目１-b)柔軟性が高く検証可能な属性提示方法（学校法人早稲田大学）
研究開発項目１-c)信頼性の高い位置情報の生成・記録（学校法人早稲田大学）
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
（ジャパンデータコム株式会社）

（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	5	3
	外国出願	0	0
外部発表等	研究論文	2	2
	その他研究発表	19	10
	標準化提案・採択	0	0
	プレスリリース・報道	0	0
	展示会	1	1
	受賞・表彰	3	3

（7）具体的な実施内容と最終成果

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方法のための要素技術研究

研究開発項目１-a)通信効率性の高い認証方法：

- アグリゲートメッセージ認証技術による相手認証技術の構築：共通鍵暗号基盤に基づくエンティティ認証技術の枠組みで、世界で初めて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提案し、その実現法としてアグリゲートメッセージ認証方式とグループテストアルゴリズムを組み合わせることによる構成法を研究開発した。さらに、これら技術を発展させ、アグリゲート相手認証（相互認証方式）や、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についても検討した。
- アグリゲート署名技術による相手認証技術の構築：公開鍵暗号基盤に基づくエンティティ認証技術の枠組みで、世界で初めて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提案し、その実現法としてアグリゲート署名方式とグループテストアルゴリズムを組み合わせることによる構成法を研究開発した。この構成法は、量子コンピュータでも計算困難な問題を利用して構成可能であるため、将来の量子コンピュータ時代においても安全なアグリゲート相手認証技術を構築できたと言える。

研究開発項目１-b)柔軟性が高く検証可能な属性提示方法

- W3C における DID と VC 方式を調査、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
- 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として、2 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
- 同じ属性を持っている相手に対する鍵共有による暗号通信機能を実装
- 概念実証(PoC)では、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。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
- 今後は、継続して W3C の標準化活動など普及に向けた展開をすすめる。

研究開発項目１-c)信頼性の高い位置情報の生成・記録

- 位置情報の生成では、機械学習による GNSS 位置情報の偽装検知を開発し、高い性能(適合率 0.97、再現率 0.93)と処理時間 1m 秒以内の完了を確認。また、将来の位置予測技術を試作し、GNSS 位置情報の偽装検知時における代替位置情報の生成を検討
- 位置情報の記録では、時系列データのメッセージ認証手法を試作、想定するユースケースに対する問題発生ゼロを確認

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

- 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、大規模環境下の衝突防止シナリオにおいて片道 40ms および往復 100ms、また、2シナリオにおいて 66%以上の帯域削減、それぞれの目標性能の実現可能性を確認した。
- 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した。
・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した。
・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、早稲田オープンイノベーションフォーラムでの展示などにより、社会認知・普及活動を展開した。

（8）研究開発成果の展開・普及等に向けた計画・展望

①計画

本研究開発終了後には研究開発で得た成果を基に国際標準化への貢献の可能性を探ってゆく。具体的には本研究開発で実装した新しい VP データフォーマットの提案やアグリゲートメッセージ認証及びそれに基づく相手認証技術のユースケースに関する Technical Report を提出できるような国際標準機関や業界団体などを探ってゆく。

また、産業応用については、構築したデモシステムで得られた知見や EdgeTech に出展したグラレコなどを活用しながら展示会への出展を視野に成果の認知度向上に努めてゆく。さらに現在調整中の EdgeTech 訪問者との打ち合わせなどを通じて、社会実装に向けた課題の有無や引き合い企業の要望などを洗い出し、ドローン産業に限らず他の産業等での活用も視野に営業活動の推進に努める。

②展望

近未来のドローン物流・人流時代の実現に向けた研究開発の一翼を担う本研究開発課題の成果は、関連産業界のみならず広く社会にインパクトを与えるものと期待している。

また、Beyond５G 時代への新たな無線通信時代に向けても、その活用の可能性を具体的事例として示しつつ、その事例に組み込んだ Beyond5G 通信網の効率的利用を可能とする技術は、電波リソースの有効活用を可能とし国民的利益に資するもの、と期待している。

今後の展望として、本研究で得られた成果展開にむけて、今後の運送業やドローン産業の動向、取り巻く市場状況やその時々の情勢を注視しながら、用途を限定せず、IoT 分野や自動車等、他分野での応用を視野に成果展開の可能性を探っていきたい。