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

令和　５ 年　 ６ 月　 ２ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１９２０

研究課題名（和文）セキュリティとリアルタイム性要求を保証した車載制御ネットワークの最適化設計

研究課題名（英文）Security-aware optimization design for in-vehicle network with guaranteed real-time requirement

研究代表者
曾　剛（ZENG, GANG）

名古屋大学・工学研究科・講師

研究者番号：９０４５６６３２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：近年、制御系車載ネットワーク（以後IVNとする）のセキュリティ脅威事例が多数指摘されている。IVNのセキュリティ強化機能を搭載する際の課題は、車載計算機のリソースの確保とリアルタイム性の保証の両立であり、そのため、本研究では複雑なIVNを対象に、以下３つの研究成果により、（１）IVNのセキュリティ要求分析とその強化技術の開発、（２）セキュリティを考慮したIVNの最適化設計手法の提案、（３）セキュリティ強化策によるIVNのリアルタイム性への影響と対策の提案、IVNのセキュリティ対策の強化とリアルタイム性の保証を同時に実現できるIVNの設計手法を研究開発した。

研究成果の学術的意義や社会的意義
本研究では、益々複雑になるIVNのメッセージの最大遅延時間解析の基礎理論から、実際の自動車に適用可能なセキュリティ強化機能とIVNの最適化設計手法の開発を実施した。理論的な研究から実用化までを目指し、実用的なセキュリティモデルと実際のIVNの特徴を考慮しながら、研究を進めた。新規性と実用性の高い研究成果により、学術的な価値に加え、自動車産業に対する波及効果も大きいと考えられる。

研究成果の概要（英文）：In recent years, numerous security threat cases have been identified in the field of In-Vehicle control Network (IVN). The challenge in implementing security enhancements in IVN lies in the simultaneous achievement of low-cost implementation on ECU and real-time guarantees. This study focuses on complex IVN systems and aims to design an IVN that ensures both security reinforcement and real-time guarantees through the following three research achievements: (1) security requirement analysis of IVN and development of corresponding security enhancement techniques, (2)proposal of design methods for IVN optimization considering security aspects, and (3) investigation of the impact of security enhancements on real-time performance in IVN and proposal of countermeasures. The research considers practical security models and the characteristics of real-world IVN. The obtained results are expected to contribute to academic research and have significant implications for the automotive industry.

研究分野：情報ネットワーク

キーワード：in-vehicle network　security measure　real-time system　optimization design　controller area network

１．研究開始当初の背景

近年、先進運転支援機能の普及や自動運転技術の進歩につれて、車載制御ネットワーク（IVN: In-Vehicle Network）が益々大規模化しており、IVN につながる制御用コンピュータである ECU（Electronic Control Unit）の数や、通信ネットワーク（バス）の本数及び転送するメッセージの数は急激に増加している。一方、IVN 経由でのなりすましメッセージや ECU のソフトウェアを不正なプログラムに書き換えるなどのセキュリティ脅威事例が多数報告されており、セキュリティ強化が必須とされている。しかしながらその一方で、車載組込みシステムでは、高度な暗号演算を実現するために高価なマイクロコントローラを採用することは、コストの観点から難しい。さらに、セキュリティ対策によるシステムのリアルタイム性に対する影響も解明されていない。このため、低コストのセキュリティ強化対策技術の実現や、セキュリティ強化を実現しつつリアルタイム性を保証するための IVN の最適化技術が重要となる。

２．研究の目的

申請者らの研究グループを含む国内外の研究者は、これまでに行われてきた研究では、IVN の最適化設計と IVN のセキュリティの 2 つテーマを分けて、別々に研究している。そのため、セキュリティ対策による IVN のリアルタイム性への影響や、セキュリティを考慮した IVN の最適化設計はまだ行われていない。また、これまでの研究ではセキュリティ要求とリアルタイム性を同時に保証することが十分に検討されていない。このため、本研究では、セキュリティ対策による IVN のリアルタイム性への影響を解明し、セキュリティ要求とリアルタイム性要求を考慮した IVN の最適化設計手法を提案する。

３．研究の方法

本研究は、複雑な制御系車載ネットワーク（IVN）を対象に、セキュリティ要求とリアルタイム性を考慮した IVN の最悪応答時間の解析手法と IVN の最適化設計手法の開発を目標として、以下 3 つのテーマで研究を行った。(1)IVN のセキュリティ要求分析とその強化技術の開発、(2)セキュリティを考慮した IVN の最適化設計手法、(3)セキュリティ強化策による IVN のリアルタイム性への影響と対策。

４．研究成果

（１）IVN のセキュリティ要求分析とその強化技術の開発

車載 CAN のセキュリティ機能を強化するために、デジタルウォーターマークとハフマン符号化に基づくセキュリティ方法を提案した。新しい方法は、比較的低い計算コストで車載ネットワークのリアルタイム要件を満たしながら、メッセージ認証の高い精度を確保することができる。CAN バスの特性を分析し、CAN メッセージにデジタルウォーターマークの挿入および抽出アルゴリズムを設計した。さらに、MAC(Message Authentication Code)の圧縮にハフマン符号化を採用することで、ECU のストレージリソースを節約し、メッセージ認証の遅延を最小限に抑えることができる。実験結果では、異なる攻撃モデルでも、提案方法がリアルタイム性を保証しながら、帯域消費が少ないことで高いメッセージ認証精度を達成できた。また、実際の CAN 通信ボードで評価し、既存の方法と比較してより高い検出精度、低い遅延、および良好な CAN との互換性を有することが検証された。この研究成果は“A Digital Watermark Method for In-Vehicle Network Security Enhancement”というタイトルで IEEE Transactions on Vehicular Technology で掲載された。

2021 年には自動車のサイバーセキュリティ強化に関する国際標準規格 ISO/SAE21434 が策定された。このため、自動車に車載侵入検知システム IDS(Intrusion Detection Systems)を搭載する際にもこの国際標準規格を満たすことが要求されている。本研究では下記３つのテーマ：IDS の要求分析、新たな IDS 方法及び IDS の評価プラットフォームを分けて、研究を行った。（１）IDS に求められる要求を具体化し、車両の安全性を満たすための要件について導出しそれらを実装するための手段について提案した。成果を国内研究会で「攻撃手法のリスク分類と車載 IDS アルゴリズムの適性評価」と「ISO/SAE 21434 プロセスを踏まえた車載 IDS の要件分析」というタイトルで発表した。（２）より柔軟な異常検知処理を実現するために、時系列データベースを用いた車載 CAN の侵入検知システム（IDS）を提案した。従来の侵入検知アルゴリズムに関する処理をクエリによる記述方法を検討した上、仮想マシン上で評価した。既存手法との比較により、実運用上の実現可能性と課題を明らかにした。これにより、攻撃の兆候が検出された自動車内に配置される IDS の侵入検知アルゴリズムをリプログラミングすることなく、チューニング可能なシステムの実現方法を示した。成果を国内研究会で「時系列データベースを用いた CAN の侵入検知システムの提案」というタイトルで発表した。（３）CAN ネットワークにおける攻撃手法のリスク分類と IDS アルゴリズムの適性評価を行った。さらに、車両外部からの不正アクセスに対する強制アクセス制御方式を提案した、また、既存の侵入検知アルゴリズムの正当性と妥当性を評価するために、侵入検知システム評価プラットフォームを提案した。成果を国内研究会で「車

載制御ネットワーク向け IDPS 評価プラットフォームの提案」というタイトルで発表した。
IVN にも Ethernet が適用されることが想定されており、サービス指向通信が導入されることが検討されている。IVN におけるサービス指向通信を実現する上での脅威について網羅的に指摘した研究はないことが課題である。このため、本研究ではサービス指向通信を用いることで実現される脅威に対する防御機構の初期検討を行った。これにより、IVN に適した強化策を提案し、従来までにはない新たな技術課題について議論した。成果を国内研究会で「車載制御システム向けサービス探索の脅威と保護手法」というタイトルで発表した。
セキュリティテストの効率を向上するための自動テスト生成方法を提案した。形式化された機能要件からのテストシナリオ生成方法を提案したと共に、外部攻撃によって危険な状態につながるテストシナリオも自動的に生成される方法を提案した。この結果、従来に比べてより多くの成立可能で重要な攻撃可能パスを導出することができた。成果を国際会議で“A Simultaneous Attack Scenario Generation Method Using the Parallel Behavior Model”というタイトルで発表した。
車載制御システム向けプロトコル SOME/IP の脅威と保護手法を分析し、その中でリアルタイム性の担保や実現性が難しいという課題が明らかにした。さらに、SOME/IP-SD メッセージを対象にグレーボックスファジングを実施し、カバレッジの評価とクラッシュの検出結果により、ソースコードの安全性を向上した。成果を国内研究会で「SOME/IP プロトコルスタックに対するグレーボックスファジングの評価」というタイトルで発表した。

（2）セキュリティを考慮した IVN の最適化設計手法
車載 IVN の最適化設計を実現するためには、通信と計算の相互作用を考慮する必要がある。例えば、通信コストを削減するため、違う周期の信号（シグナル）を一つのメッセージにパッキングすることがある。しかしながらその一方で、そのメッセージを受信する ECU では必要以上の割り込み MRI(Message Receiving Interrupts)が発生することで、計算コストが高くなることやリアルタイム性に悪影響を与えることがある。また、車載 CAN FD(Controller Area Network with Flexible Data Rate)の設計に関する既存研究では、通信の帯域利用率の最小化のみを考慮し、メッセージ受信割り込みの発生が無視されていた。この問題を解決するために、私たちは CAN-FD の帯域利用率の最小化と不必要な MRI の数の最小化という矛盾する問題を最適化問題として定式化した。まず、メッセージによって引き起こされる不必要な MRI の数を分析するアルゴリズムを提案し、次に、中規模の信号セットに対してはトップダウンアプローチ、大規模な信号セットに対してはハイブリッドアプローチという 2 つのヒューリスティックアルゴリズムを提案し、上記の最適化問題を解ける。実験結果では、既存のアルゴリズムと比較して、帯域利用のオーバーヘッドが少ないことで不必要な MRI を大きく削減できることを示された。この研究成果は“Balancing Bandwidth Utilization and Interrupts: Two Heuristic Algorithms for the Optimized Design of Automotive CPS”というタイトルで IEEE Transactions on Industrial Informatics で掲載された。
自動車の CASE 化や、ソフトウェア定義車などの発展が期待されている。このため、車載ネットワークには拡張性のある設計が要求されており、自動車の E/E アーキテクチャの設計において重要な設計目標になっているものの、まだ十分に考慮されていない。この課題に対処するために、私たちは CAN FD の信号パッキングにおける帯域利用率の最小化と拡張性の最大化というトレードオフ問題を最適化問題として定式化し、以下 3 つのコア技術の提案により拡張性を考慮した車載ネットワークの最適化設計技術を開発した。より具体的には、（1）与えられたメッセージセットの拡張可能性を定量的に測定するために、3 次元の拡張性モデルと関連する拡張性メトリックを新たに提案した。（2）中規模の信号セットに適した拡張性を考慮した信号パッキング問題を解決するために、MILP(Mixed Integer Linear Programming)ベースのアプローチを提案した。（3）産業用の大規模信号セットを設計するために、焼きなまし法(SA)ベースのヒューリスティックメソッドを提案した。実験では、既存のアルゴリズムと比較して、少ない増加した帯域で、拡張された信号セットの送受信ができることが確認された。この研究成果は、“Optimizing Extensibility of CAN FD for Automotive Cyber-Physical Systems”というタイトルで IEEE Transactions on Intelligent Transportation Systems で掲載された。
STRIDE のガイドワードに対し、CAPEC の攻撃手法の情報を紐づけることで、より具体的な脅威シナリオを特定する手法を提案した。特定された脅威シナリオの件数増加やシナリオの具体性向上といった結果から、提案手法の有用性を示した。今後は自動車の脆弱性がセンサー情報の性能限界から起こりること、従来のソフトウェア上の脆弱性とは異なるシステム上の欠落点から、自動車の安全性が侵害されること、さらにはこれらのデータベースの整備について提案した。成果を国内研究会で「自動車向け CAPEC の検討と脅威シナリオ特定への活用」というタイトルで発表した。
車載インフォテインメントシステムにおける電磁的記録を活用することで、攻撃の全体像に関わる電磁的記録を補完できる可能性を示した。今後 CAN の実データに関する情報を取得する仕組みを実装することで、デジタル・フォレンジックの精度をより向上させることが可能であることを示した。成果を国内研究会で「車載システムに対するデジタル・フォレンジックに向けての一考察」というタイトルで発表した。

（3）セキュリティ強化策による IVN のリアルタイム性への影響と対策

CAN FD は､高いビットレートとメッセージペイロードが大きいという二つの利点を持つため、有望な車載ネットワークとして注目されている。CAN FD を潜在的なセキュリティ攻撃から保護するために、HSM(Hardware Security Module)ベースのセキュリティ対策が推奨されているが、HSM の導入によって CAN FD のリアルタイム性（メッセージの送信時間）にどういう影響を与えているかまだ解明されていない。そのため、私たちは、セキュリティ対策（HSM の導入）によるメッセージの送信時間における影響について解析した。具体的に、まず、HSM による CAN FD メッセージの処理過程をモデル化して、次に、メッセージの最悪応答時間(WCRT)の解析方法を提案した。さらに、WCRT の解析結果が CAN FD メッセージの真の最悪応答時間をバウンドすることを理論的に証明した。最後に、提案の解析方法を用いて、HSM によりメッセージのリアルタイム性に対する影響を実験で調べた。この研究により、HSM を搭載している ECU におけるリアルタイム性の解析ができるようになった。この研究成果は“Timing Analysis of CAN FD for Security-Aware Automotive Cyber-Physical Systems”というタイトルで IEEE Transactions on Dependable and Secure Computing に掲載された。

セキュリティ対策の通信コストを削減するために、すべてのメッセージにメッセージ認証コード（MAC）を割り当てることなく、Keep Alive Messages を利用した攻撃検知手法を提案した。これにより、各メッセージに認証情報をつけることなく、リアルタイム性を満たしながらセキュリティを確保するための方法について提案した。この結果、より少ない帯域でリアルタイム性を保証しながらセキュリティを確保することを実現した。成果を国際会議で“Towards Minimizing MAC Utilization for Controller Area Network”というタイトルで発表した。

実際の IVN では ECU が各 CAN メッセージの遅延時間を知る方法がない。この課題に対処するために、各 ECU ノード間のグローバル時間に同期せずに、各メッセージの実際の遅延時間を受信ノートに通知することができる DDCAN（Delay-time Deliverable CAN）を提案した。これにより、なりすましメッセージであるかどうかを判断することが容易になる可能性があることを議論した。成果を国際会議で“DDCAN:Delay-time Delivable CAN network”というタイトルで発表した。

これまで IVN にはアクセス制御機構がないため、攻撃者により接続された機器を認証や認可を与えることなく、IVN にアクセスすることができた。このため、本研究では IVN に対するアクセス制御機構を提案した。このアクセス制御機構では、各 ECU が自身に与えられる制御データの送信のみが許可されるような制御機構を実装することで、後から入ってくる攻撃者を排除することが可能となる。この結果、従来よりも堅牢で集中的なアクセス制御を実行することを可能とした。成果を国内研究会で「車載制御システム向け強制アクセス制御機構の提案」というタイトルで発表した。

セキュリティ対策とリアルタイム性のトレードオフを実現するため、SOME/IP-SD の拡張プロトコルを提案した。通信オーバーヘッドを低減するだけではなく、セキュリティ保護レベルを導入することにより、様々な保護手段を動的に変更できる能力があった。今後は自動車のソフトウェアプラットフォームの標準化団体である AUTOSAR への研究成果の提案について議論する予定である。成果を国内研究会で「SOME/IP-SD のセキュリティ拡張プロトコルの提案」というタイトルで発表した。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　4件／うちオープンアクセス　0件）

１．著者名 Wufei Wu, Junhao Dai, Huijuan Huang, Qinmin Zhao, Gang Zeng and Renfa Li	４．巻 2
２．論文標題 A Digital Watermark Method for In-Vehicle Network Security Enhancement	５．発行年 2023年
３．雑誌名 IEEE Transactions on Vehicular Technology	６．最初と最後の頁 1-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TVT.2023.3247180	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yong Xie, Gang Zeng, Ryo Kurachi, Fu Xiao, Hiroaki Takada and Shiyan Hu	４．巻 7
２．論文標題 Timing Analysis of CAN FD for Security-Aware Automotive Cyber-Physical Systems	５．発行年 2022年
３．雑誌名 IEEE Transactions on Dependable and Secure Computing	６．最初と最後の頁 1-14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TDSC.2022.3194712	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yong Xie, Gang Zeng, Ryo Kurachi, Fu Xiao, and Hiroaki Takada	４．巻 22
２．論文標題 Optimizing Extensibility of CAN FD for Automotive Cyber-Physical Systems	５．発行年 2021年
３．雑誌名 IEEE Transactions on Intelligent Transportation Systems	６．最初と最後の頁 7875-7886
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TITS.2021.3059769	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yong Xie, Gang Zeng, Ryo Kurachi, Xin Peng, Guoqi Xie, and Hiroaki Takada	４．巻 16
２．論文標題 Balancing Bandwidth Utilization and Interrupts: Two Heuristic Algorithms for the Optimized Design of Automotive CPS	５．発行年 2020年
３．雑誌名 IEEE Transactions on Industrial Informatics	６．最初と最後の頁 2382-2392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TII.2019.2936240	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　4件）

１．発表者名
金森健人、棚原斎稀、渡邉弘樹、平野雅巳、新垣奈美子、鉢嶺光、倉地亮

２．発表標題
SOME/IPプロトコルスタックに対するグレーボックスファジングの評価

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2023)

４．発表年
2023年

１．発表者名
小野華、倉地亮、土居元紀、岩原主、前田和輝、渡邊謙一郎

２．発表標題
自動車向けCAPECの検討と脅威シナリオ特定への活用

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2023)

４．発表年
2023年

１．発表者名
倉地亮、高田広章、足立直樹、上田浩史

２．発表標題
SOME/IP-SDのセキュリティ拡張プロトコルの提案

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2023)

４．発表年
2023年

１．発表者名
倉地 亮、高田 広章、足立 直樹、上田 浩史、宮下 之宏

２．発表標題
時系列データベースを用いたCANの侵入検知システムの提案

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名
倉地亮、佐々木崇光、氏家良浩、松島秀樹

２．発表標題
ISO/SAE 21434プロセスを踏まえた車載IDSの要件分析

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名
味岡 仁雅、倉地 亮、佐々木 崇光、黒崎 雄介、片山 隆成、下雅意 美紀

２．発表標題
車載システムに対するデジタル・フォレンジックに向けての一考察

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2022)

４．発表年
2022年

１．発表者名
Toshiyuki Fujikura and Ryo Kurachi

２．発表標題
A Simultaneous Attack Scenario Generation Method Using the Parallel Behavior Model

３．学会等名
2020 IEEE 91st Vehicular Technology Conference(VTC2020-Spring)（国際学会）

４．発表年
2020年

１．発表者名
倉地亮，高田広章，足立直樹，上田浩史，滝本周平

２．発表標題
車載制御システム向けサービス探索の脅威と保護手法

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2021)

４．発表年
2021年

１．発表者名
倉地亮，佐々木崇光，氏家良浩，松島秀樹

２．発表標題
攻撃手法のリスク分類と車載IDSアルゴリズムの適性評価

３．学会等名
暗号と情報セキュリティシンポジウム(SCIS2021)

４．発表年
2021年

１．発表者名
Shan Ding, Hui Wang, and Gang Zeng

２．発表標題
An Integrated Framework for Packing CAN-FD Frames and Assigning Offsets

３．学会等名
IEEE Smart World Congress（国際学会）

４．発表年
2019年

１．発表者名
Ryo Kurachi, Hiroaki Takada, Naoki Adachi, Hiroshi Ueda

２．発表標題
DDCAN: Delay-time Delivable CAN network

３．学会等名
IEEE International Workshop on Automobile Software Security and Safety（国際学会）

４．発表年
2019年

１．発表者名
Ryo Kurachi, Hiroaki Takada, Hiroshi Ueda, Shuhei Takimoto

２．発表標題
Towards Minimizing MAC Utilization for Controller Area Network

３．学会等名
The 2nd ACM Workshop on Automotive and Aerial Vehicle Security（国際学会）

４．発表年
2019年

１．発表者名 倉地亮、佐々木崇光、前田学、安齋潤、松島秀樹
２．発表標題 車載制御ネットワーク向けIDPS評価プラットフォームの提案
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2020)
４．発表年 2020年

１．発表者名 倉地亮、高田広章、足立直樹、上田浩史、滝本周平
２．発表標題 車載制御システム向け強制アクセス制御機構の提案
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2020)
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	倉地　亮 (KURACHI RYO) (10568059)	名古屋大学・情報学研究科・特任准教授 (13901)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関