博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　Anomaly Detection Technology for In-vehicle Networks
申請者　：　矢嶋　純
審査委員会　：　主査　教授　大久保 隆夫
副査　教授　松井 俊浩
副査　准教授　橋本 正樹
副査　准教授　稲葉 緑

Ⅰ．論文内容の要旨

自動車へのサイバー攻撃は、人命に関わる大問題であるため、様々なセキュリティ技術を利用して守るべきであると考えられる。例えば多層防御（Multi-layered security）の考え方で、自動車の外部から内部に至るまでの侵入経路にそれぞれセキュリティ機能を設置することや、多重防御（Defense in depth）の考え方で、制御系装置を監視し、それらの接続先を認証し、ログを取得して分析することなどを検討する必要がある。また、セキュリティマネージメントサイクルを回す運用も行う必要があると考えられる。本論文では、数あるセキュリティ技術の中でも車載ネットワーク、特に CAN における攻撃検知技術に焦点を当てている。CAN のメッセージは、送信間隔に応じて、Periodic messages (Perfectly periodic / Quasi-periodic)、Event-based messages、Non-periodic messages の 3 種に分類される。

筆者は、Perfectly periodic messages と Quasi-periodic messages に対する攻撃検知が重要だと考え、これらのメッセージに対する攻撃を高精度に検知できる手法を考案することとした。それが提案 1 (Anomaly Detection by Cumulative Sum 法)である。また、残りのメッセージについても数十パーセントを占めており、無視することはできない。提案 2 （Single Message Format Estimation 法）と提案 3 （Data Relation Analysis 法）はこれらのメッセージを含む全てのメッセージタイプに対する攻撃を検知する手法を構築するために役立つ手法である。

第 1 章では、背景、本研究の目的、各章の構成について述べている。近年、外部からの遠隔操作攻撃が懸念されていることから、車載向けセキュリティ対策の重要性が高まっている。本論文では、数あるセキュリティ技術の中でも車載ネットワークにおける攻撃検知技術に焦点を当てると述べている。

第 2 章では、乗り物に対するサイバー攻撃について直接攻撃と間接攻撃の 2 種類に分けて概観している。その上で、本研究では間接攻撃について主に扱うとしている。

第 3 章では、一般的なセキュリティ戦略について、マルチレイヤ、多層防御、マネジメントサイクルの観点から述べている。マネジメントサイクルは、Identity、Protection、Detection、Respond、Recovery の要素で構成される。このうち本論文では Detection(検知)について主に扱うと述べている。

第 4 章では、車載システムに対するセキュリティの先行研究とその課題について述べている。車載ネットワークは専用プロトコルを利用しており、その仕様の特異性から、一般の IT 向け（TCP/IP 向け）の攻撃検知がそのまま利用できない。また、既存の車載向け攻撃検知にも課題があるとしている。

第 5 章では、車載ネットワーク、特に CAN と CAN に流れるメッセージの形式と特徴について

述べている。本研究では、現在の車載ネットワークプロトコルの主流が CAN であることから、CAN 経由の攻撃検知の前提となる CAN メッセージの形式、特徴について述べている。

第 6 章では、CAN のメッセージの既存のアノマリ検知について、ルールベースの検知、非ルールベースの検知について述べている。また、検知手法に求められる要件と既存手法の課題を挙げ、それに対し筆者の提案するアプローチの概要を説明している。

第 7 章では、筆者の 3 つの提案のうちの Anomaly Detection by Cumulative Sum 法、周期に着目し累積和を用いた検知手法について紹介している。既存の周期に着目した検知では受信間隔が少しでも周期から逸脱すると誤検知の可能性があった。本研究の手法は周期から多少逸脱しても誤検知を生じないよう、受信開始からのその CAN-ID を持つメッセージの想定受信数を毎周期導出し、実際の受信数と比較して検知する。攻撃があれば実際の受信数のほうが上回るはずだが、直ちに攻撃と判定してしまうと正常メッセージが早着したのかを区別することができないため、判断を一旦保留し、その状態が次の周期まで継続するようであれば攻撃として検知する手法とした。

第 8 章では、Single Message Format Estimation 法のメッセージ形式の予測を行う手法について述べている。メッセージ内容に着目した検知を行う場合、ペイロード内の field-data のフォーマットを知っていると高精度な検知を実現できると考えられる。既存の手法では 5 つの field-data のタイプを予測することが可能であったが、本研究では 10 種類のタイプを予測可能にする新しいフォーマット予測技術を提案した。

第 9 章では Data Relation Analysis 法の、メッセージ同士の相関関係に基づいたアノマリ検知手法について述べている。Data Relation Analysis 法では異なる field-data 間の関連性を発見する方法を実現することより上で述べた方法とは別の検知手法が実現できるようになり、検知精度は向上すると考えられる。提案手法では，event-based periodic messages に着目し、このメッセージの特徴である「イベント発生時に値が特定の値になる」ケースと、「イベント発生時に値が変化する」ケースを複数発見し関連のある field-data を見つける。

第 10 章では、実車のログデータを用いて提案手法の評価を行い、一部は先行研究と比較を行った上で、高い精度を得られたことを述べている。Anomaly Detection by Cumulative Sum 法については実験を行い、既存の手法と比べて攻撃検知精度が極めて高いことを確認した。Single Message Format Estimation 法では、実験を行い、既存の手法よりも高精度に予測できることを確認した。また予測結果を用いて機械学習ベースの検知を行った場合、フォーマットを知らない場合と比べて検知精度が高くなることを確認した。Data Relation Analysis 法では、実験により、実自動車のログから、そのようなメッセージを発見することができ、検知に応用できることが分かった。

第 11 章では、Anomaly Detection by Cumulative Sum 法、Single Message Format Estimation 法、Data Relation Analysis 法を用いた検知の例を紹介している。例では、Single Message Format Estimation 法、Data Relation Analysis 法で得られた知見を基にルールベースの検知を実装し、実際の検知精度について評価している。

第 12 章では、提案手法の有効性について議論を行っている。議論では、各提案手法に対して想定される攻撃を挙げ、耐性について述べている。また、本提案の利点と課題について述べている。また、実際に攻撃を検知した場合、車の制御にどのように対応させるかや、理想的なネットワーク構成について議論している。

第 13 章では、結論と今後の課題について述べている。今回の 3 つの提案により、自動車のすべての送信方法に対応した攻撃検知が実現可能となった。それぞれの性能についても従来よりも向上していることが確認できたとしている。

情報セキュリティ大学院大学　情報セキュリティ研究科

Ⅱ. 論文審査結果の要旨

本論文は、自動運転が進む中、確実に脅威になることが想定される車載システムへのサイバー攻撃に対処するため、その検知に焦点を当て、メッセージの特徴をふまえた上で 3 つの手法による、とりこぼれのない検知手法を提案している。各提案手法は検証によって高い精度が確認できており、より実際的な、かつ社会にとって有用な技術である。

よって、本論文は、博士（情報学）の論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、2021 年 1 月 13 日に口述諮問と最終試験審査、1 月 30 日に発表会を行った。審査に当たっては、博士学位のディプロマ・ポリシーに基づいて総合的に評価した。審査委員から、検証のためのデータに偏りがある点について改善コメントがあり、より一般性の高い追加データによる検証を行うなど、論文の改善を行ってもらったことを 2 月 24 日の最終試験審査で確認し、申請者が学位取得にふさわしい知見を持つものと判断した。