イベント送信付き周期型 CAN 通信に適した ルールベース異常検知

松林 勝[1,*] 小山 卓麻[1] 岡野 靖[1] 田中 政志[1] 宮島 麻美[1]

概要：自動車の制御通信プロトコルとして Controller Area Network (CAN) がある．この CAN の通信に対してのメッセージ挿入攻撃を検知する手法が多く提案されている．その中には，周期的な送信方式とイベントドリブンな送信方式が混在する「イベント送信付き周期型 CAN 通信」を対象とした手法がある．その手法は，CAN メッセージの送信間隔やペイロードの値・変化量などの正常性を学習し，学習した正常性を基に異常検知を行っている．しかしペイロードの値・変化量のバリエーションは多く，その正常性を網羅的に学習するコストが高い．また学習漏れにより，False Positive (FP) が多く発生するという問題もその手法には存在する．そこで本研究では，イベント送信付き周期型 CAN 通信を分析し，バリエーションの多い特徴量の学習を行わずとも高精度で挿入攻撃を検知するのに有効な 3 つの特性を明らかにした．提案手法ではその特性をルール化し，そのルールを用いてイベント送信付き周期型 CAN 通信への挿入攻撃を検知する．実車に対して挿入攻撃を実施しつつ収集したデータを用いた評価により True Positive Rate = 97.26%，FP Rate = 0.0002%を実現できたことを示す．

キーワード：Controller Area Network，イベント送信付き周期送信，挿入攻撃，ルールベース異常検知

Rule-Based Anomaly Detection for Mixed Interval (Periodic/ Sporadic) CAN Messages

Masaru MATSUBAYASHI[1,*] Takuma KOYAMA[1] Yasushi OKANO[1]
Masashi TANAKA[1] Asami MIYAJIMA[1]

Abstract: Controller Area Network (CAN) is a communication protocol used in vehicle control networks. It has been proposed that methods for detecting message injection attacks into CAN messages. Some of these are methods for detecting message injection attacks into mixed interval CAN messages that include periodic and sporadic transmissions. These methods detect anomalous CAN messages by learning normality of transmission intervals, payload values, and payload changes of mixed interval CAN messages. However, a cost of learning the normality is high because there are many variations of payload values and payload changes. Besides, these methods produce many false positives (FPs) due to learning deficiency of the normality. We reveal three characteristics, which are effective to detect message injection attacks with high detection performance without learning normality of features that have many variations. Our proposed method defines rules based on the three characteristics and detects message injection attacks into mixed interval CAN messages by using the defined rules. We evaluate the proposed method by using data collected from real vehicles. Our result shows that the proposed method achieved high detection performance: a true positive rate of 97.26% and a FP rate of 0.0002%.

Keywords: Controller Area Network, mixed interval (periodic/ sporadic), injection attack, rule-based anomaly detection

1. はじめに

多くの自動車には，制御通信プロトコルである Controller Area Network (CAN) [1]で規定されるネットワークが搭載されている．CAN はバス型のネットワークであり，多くの電子制御装置 (ECU) を接続している．各 ECU は，CAN に対してメッセージ（CAN メッセージ）をブロードキャストすることで相互に通信を行っている．この CAN メッセージは，CAN メッセージの種別を示す CAN-ID と最大 8 バイトのペイロードなどで構成されている．一方で，CAN メッセージには送信元や宛先の情報が含まれない．また，メッセージ認証の機能もない．そのため，不正な送信元から不正な CAN メッセージを送信する攻撃（挿入攻撃）により，容易に自動車を不正制御できることが示されている[2-4].

これまで，CAN 通信に対しての挿入攻撃を検知する手法が多く提案されている[5,6]．特に，周期型 CAN 通信に対しての挿入攻撃を検知する手法[7-9]が多く提案されている．周期型 CAN 通信とは，1 種類の CAN-ID に着目したときに CAN メッセージが一定間隔（周期間隔）で送信（周期送信）されている CAN 通信である．先行研究[7-9]の手法は，挿入攻撃が発生した際に周期型 CAN 通信の周期性が崩れることを利用して挿入攻撃を検知している．

一方，イベント送信付き周期型 CAN 通信に対しての挿入攻撃の検知に適した手法[10-14]も提案されている．イベント送信付き周期型 CAN 通信は，1 種類の CAN-ID に着目

1 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
* masaru.matsubayashi.tv@hco.ntt.co.jp

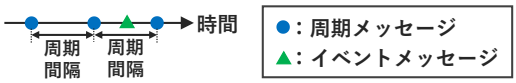


図 1　イベント送信付き周期型 CAN 通信の一例

したときに周期送信とイベントドリブンな送信（イベント送信）が混在している CAN 通信である．図 1 に周期送信された CAN メッセージ（周期メッセージ）とイベント送信された CAN メッセージ（イベントメッセージ）の関係を示す．図 1 に示す通り，イベントメッセージと直前の CAN メッセージの送信時刻の差（送信間隔）は周期間隔よりも短くなる．そのため，CAN 通信の周期性が崩れることを利用して挿入攻撃を検知する先行研究[7-9]の手法では，イベントメッセージを誤って異常と判定してしまう可能性がある．

それに対して先行研究[10-14]は，送信間隔やペイロードの値，ペイロードの変化量の正常性を学習し，その正常性を基に異常検知を行う手法を提案している．しかし，ペイロードの値や変化量のバリエーションは多いため，このことを原因とした 2 つの問題が先行研究[10-14]に存在する．1 つ目はその正常性を網羅的に学習するコストが高いという問題である．2 つ目は，その正常性の学習漏れが発生した場合に，正常な CAN メッセージを異常と誤判定した False Positive (FP) が多く発生するという問題である．

そこで本研究では，前述の 2 つの問題の原因を解決する．そして，イベント送信付き周期型 CAN 通信に対しての挿入攻撃を先行研究より低い FP Rate (FPR) かつ先行研究と同等の True Positive Rate (TPR) で検知可能な手法を実現することを目的とする．その目的の達成に向け，実際の自動車に対して挿入攻撃を実施しつつ収集したイベント送信付き周期型 CAN 通信ログの分析を行った．なお，CAN 通信ログは CAN メッセージとその受信時刻を合わせたログと定義する．分析の結果，ある 2 つの CAN メッセージのペイロードの特定バイト位置（ペイロードの対象部）の値が同一か否かと，それらの送信間隔が周期間隔か否かが挿入攻撃の有無により異なるという特性 3 つが明らかとなった．この単純な特性を利用することで，バリエーションの多い特徴量の学習を行わずとも低 FPR かつ高 TPR で挿入攻撃の検知が可能になる．

本研究では，その 3 つの特性を利用したルールを定義し，そのルールを利用して異常検知を行う手法を提案する．そして，メーカの異なる 2 車種の自動車から収集した CAN 通信ログを用いて提案手法を評価した．その評価では，イベント送信付き周期型 CAN 通信を対象とした先行研究[14]の手法と提案手法の比較評価を行った．その結果，提案手法は TPR = 97.26%（先行研究と比較して約 4.14%向上），FPR = 0.0002%（先行研究と比較して約1/154に低減）でイベント送信付き周期型 CAN 通信への挿入攻撃を検知できることを示した．

2. 関連研究

本章では，周期型 CAN 通信を対象とした異常検知手法を提案している先行研究とイベント送信付き周期型 CAN 通信に適した異常検知手法を提案している先行研究について述べる．また，それらの手法の問題点を述べる．

2.1 周期型 CAN 通信を対象とした異常検知

先行研究[7-9]は，送信間隔を検知指標としたルールにより異常検知を行う手法を提案している．例えば Gmiden ら[7]は，送信間隔が周期間隔の半分よりも短い場合は異常であるというルールにより異常検知を行っている．Moore ら[8]と Otsuka ら[9]は，周期メッセージの送信間隔が周期間隔よりもわずかに短くなるケースの存在を考慮している．そして，そのケースよりも送信間隔が短い CAN メッセージを異常と判定するルールにより異常検知を行っている．

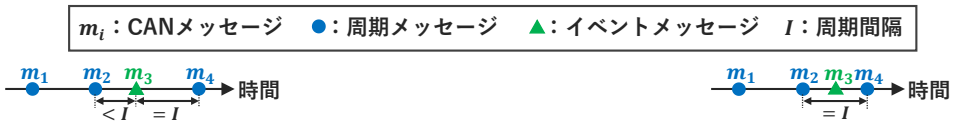
イベント送信付き周期型 CAN 通信に先行研究[7-9]を適用した場合，イベントメッセージを誤って異常と判定してしまう可能性が高い．そのため，本研究が対象としているイベント送信付き周期型 CAN 通信に対して先行研究[7-9]の手法を適用することは不適切と考える．

2.2 イベント送信付き周期型 CAN 通信に適した異常検知

先行研究[10-14]は，送信間隔やペイロードの値，ペイロードの変化量の正常性を学習し，その正常性を基に異常検知を行う手法を提案している．ペイロードから抽出した特徴量を利用することで，先行研究[7-9]の手法では困難だったイベントメッセージと攻撃者により挿入された CAN メッセージ（挿入攻撃メッセージ）の区別が可能になる．

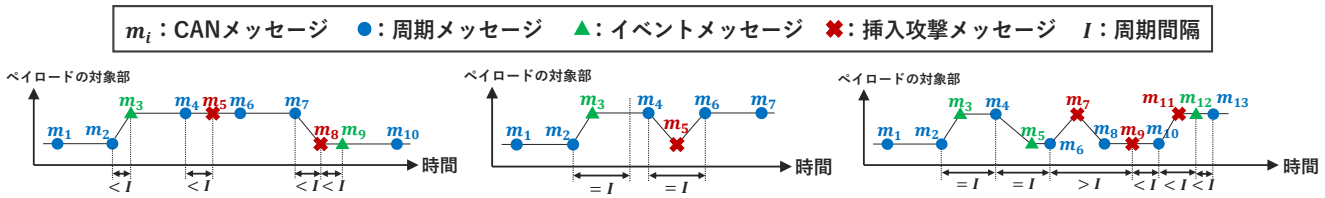
Taylor ら[10]は，一定時間で観測した複数 CAN メッセージの送信間隔やペイロードの変化量の正常値を基に異常検知を行う手法を提案している．また，Taylor ら[11]と福田ら[12]は Long Short-Term Memory を用いて次に送信される CAN メッセージのペイロードの正常値を予測し，その予測値と実測値の差を基に異常検知を行う手法を提案している．

矢嶋ら[13]と Koyama ら[14]はイベント送信付き周期型 CAN 通信を適用対象の一つに位置付けた異常検知手法を提案している．矢嶋ら[13]は，イベント送信が発生するタイミングやペイロード変化が発生するタイミングが複数の CAN-ID 間で関連していることを利用した異常検知手法を検討している．しかし，その手法の評価は行われていない．一方で Koyama ら[14]は手法の評価まで実施し，高精度で異常検知が可能であることを示している．この手法は，直近 3 つの CAN メッセージをm_i，m_{i-1}，m_{i-2}としたときのm_{i-2}とm_{i-1}の送信間隔とペイロードの変化量およびm_{i-1}とm_iの送信間隔とペイロードの変化量を 1 つのベクトルとして利用する．そして，このベクトルのホワイトリストを事前に学習し，ホワイトリストに存在しないベクトルを持つ 3 つの CAN メッセージを異常と判定している．



(a)　周期ズレあり型　　(b)　周期ズレなし型

図 2　イベント送信付き周期型 CAN 通信に存在する 2 種類の Type



(a)　特性 1　　(b)　特性 2　　(c)　特性 3

図 3　挿入攻撃の検知に有効な 3 つの特性

ペイロードの値や変化量のバリエーションが多いことが原因で，それらの正常性を網羅的に学習するコストが高いという問題が先行研究[10-14]にはある．加えて，学習漏れが発生した場合に，FP が多く発生するという問題もある．

3.　イベント送信付き周期型 CAN 通信の分析

先行研究の 2 つの問題の原因解決，ひいては本研究の目的の達成に向けて，実際の自動車に対して挿入攻撃を実施しつつ収集したイベント送信付き周期型 CAN 通信ログの分析を行った．その結果，バリエーションの多い特徴量の学習を行わずとも低 FPR かつ高 TPR で挿入攻撃を検知するのに有効と考えられる 3 つの特性を明らかにした．本章では，その分析と結果について述べる．

3.1　分析用の CAN 通信ログの収集

分析用の CAN 通信ログを国内メーカ A の車種 X の自動車から収集した．収集した CAN 通信ログは，挿入攻撃を実施せずに収集した CAN 通信ログ（4.8 時間分）と挿入攻撃を実施しつつ収集した CAN 通信ログ（25.4 時間分）の 2 種類である．これらの CAN 通信ログは，様々な自動車状態（停止や走行など）において運転中に行われ得る様々な操作(ライトやエアコンの操作など)を実施しつつ収集した．

また，挿入攻撃を実施しつつ収集した CAN 通信ログについては，挿入攻撃に関する 5 つのパラメータを様々変化させつつ収集した．1 つ目は挿入攻撃メッセージに設定する CAN-ID である．このパラメータが取る値はイベント送信付き周期型 CAN 通信を行う CAN-ID 数種類と周期型 CAN 通信を行う CAN-ID 数種類である．2 つ目は，挿入攻撃メッセージを挿入する区間に関するパラメータである．このパラメータが取る値は「変化あり区間」と「変化なし区間」の 2 種類である．なお本稿では，ある CAN メッセージとその次に送信された CAN メッセージの 2 つの関係を「隣接」と定義し，隣接したメッセージ間の時間を「区間」と定義する．また，変化なし区間とは，隣接したメッセージのペイロードが同一の区間であり，変化あり区間とは，隣接したメッセージのペイロードが異なる区間である．3 つ目は，挿入攻撃メッセージを挿入するタイミングに関するパラメータである．このパラメータが取る値は「区間の開始直後」と「区間の中間」と「区間の終了直前」の 3 つである．4 つ目は，挿入攻撃メッセージの挿入数に関するパラメータである．このパラメータが取る値は「1 メッセージ」や「2 メッセージ」などの複数種類である．5 つ目は，挿入攻撃メッセージのペイロードに関するパラメータである．このパラメータが取る値は「区間の始点に位置する CAN メッセージと同一のペイロード」と「区間の終点に位置する CAN メッセージと同一のペイロード」と「前述した 2 つ以外のペイロード」の 3 種類である．

3.2　分析結果

分析の結果明らかとなったイベント送信付き周期型 CAN 通信に存在する 2 種類の Type について述べる．また，その Type ごとに分析した結果明らかとなった，3 つの特性について述べる．

3.2.1　2 種類の Type

イベント送信付き周期型 CAN 通信には CAN-ID によって 2 種類の Type が存在することが明らかとなった．1 つ目は図 2 (a) に示す Type であり，イベントメッセージm_3とその直後の周期メッセージm_4の送信間隔が常に周期間隔となる Type である．本稿ではこの Type を「周期ズレあり型」とする．2 つ目は図 2 (b) に示す Type であり，周期メッセージm_2とm_4の送信間隔がイベントメッセージm_3の送信の有無に依らず常に周期間隔となる Type である．本稿ではこの Type を「周期ズレなし型」とする．

3.2.2　挿入攻撃の検知に有効な 3 つの特性

イベント送信付き周期型 CAN 通信には，バリエーションの多い特徴量の学習を行わずとも低 FPR で挿入攻撃を検知するのに有効な 3 つの特性が存在することが明らかとなった．図 3 はその 3 つの特性を視覚化した図であり，ペイロードの対象部の値と時間をそれぞれ縦軸と横軸として

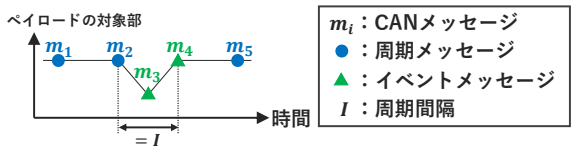


図 4　特性 2 に反する CAN 通信ログの例

CAN メッセージをプロットした図である．また，図 3 (a) と図 3 (b) は周期ズレあり型に当てはまる特性であり，図 3 (c) は周期ズレなし型に当てはまる特性である．

特性 1 は「周期間隔よりも短い送信間隔で送信されたイベントメッセージのペイロードの対象部は，隣接した直前の CAN メッセージのペイロードの対象部と異なる（図 3 (a) のm_2，m_3）．反対に，隣接した直前の CAN メッセージとペイロードの対象部が同一である CAN メッセージが周期間隔よりも短い送信間隔で送信されている場合は挿入攻撃が発生している（図 3 (a) のm_4~m_6およびm_8，m_9）．」という特性である．なお，ペイロードの対象部はペイロード全体である．

特性 2 は「イベントメッセージの前後に存在する 2 つの周期メッセージの送信間隔は周期間隔よりも長く，かつペイロードの対象部が異なる（図 3 (b) のm_2~m_4）．反対に，挿入攻撃メッセージの前後に存在する周期メッセージの送信間隔は周期間隔であり，かつペイロードの対象部が同一である（図 3 (b) のm_4~m_6）．」という特性である．なお，ペイロードの対象部はペイロード全体である．

特性 3 は「挿入攻撃が発生していなければ，ペイロードの対象部が隣接した直前の CAN メッセージと同一である CAN メッセージが周期間隔で出現する（図 3 (c) のm_2, m_4, m_6）．反対に挿入攻撃が発生すると，ペイロードの対象部が隣接した直前の CAN メッセージと同一である CAN メッセージが周期間隔で出現しなくなる（図 3 (c) のm_6~m_{13}）．」という特性である．なお，ペイロードの対象部はイベント送信時にのみ変化するバイト位置のみである．

特性 1 と特性 3 は分析用の CAN 通信ログにおいて必ず成立していた．つまり，特性 1 と特性 3 は FP を発生させずに挿入攻撃を検知するのに有効な特性である．

一方，特性 2 は分析用の CAN 通信ログのほとんどにおいて成立していたが，ごく一部において成立していなかった．具体的には，図 4 に示すイベントメッセージが分析用の CAN 通信ログのごく一部に存在しており，これが特性 2 に反していた．そのため，特性 2 を利用して異常検知を行うと図 4 に示すイベントメッセージを誤って異常と判定してしまう．しかし，様々な自動車状態において運転中に行われ得る様々な操作を実施しつつ収集した約 30 時間分のデータにおいて，図 4 に示すイベントメッセージが発生したのは数回であった．つまり特性 2 は，FP を極めて少ない数に抑えつつ挿入攻撃を検知するのに有効な特性と考える．

3 つの特性は，ある 2 つの CAN メッセージのペイロードの対象部が同一か否か，それらの送信間隔が周期間隔か否かに基づいた単純なものである．よって，この特性を利用することで，バリエーションの多い特徴量の学習を行わずとも低 FPR で挿入攻撃の検知が可能となる．

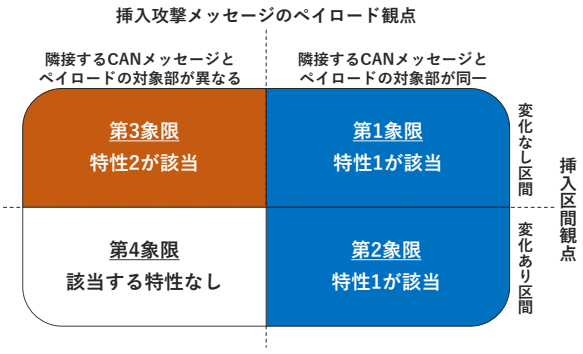


図 5　3 つの特性を利用することで検知可能な挿入攻撃メッセージの範囲（周期ズレあり型）

図 6　3 つの特性を利用することで検知可能な挿入攻撃メッセージの範囲（周期ズレなし型）

3.2.3　3 つの特性を利用することで検知可能な攻撃の考察

3 つの特性が挿入攻撃メッセージを高 TPR で検知するのに有効か，つまり挿入攻撃メッセージを漏れなく検知するのに有効かどうかについて考察する．そのために，挿入攻撃メッセージの集合を漏れなく・重複なく分割し，分割した部分集合と 3 つの特性の対応関係を示す．

挿入攻撃メッセージの集合を分割した結果を図 5 と図 6 に示す．まず挿入攻撃メッセージの集合を Type ごとに分割する．さらに Type ごとに分割した挿入攻撃メッセージの部分集合を，挿入区間観点と挿入攻撃メッセージのペイロード観点の 2 つの観点で 4 分割する．挿入区間観点では，ペイロードの対象部の変化なし区間に攻撃を挿入する場合と，変化あり区間に攻撃を挿入する場合の 2 つに分割する．そして挿入攻撃メッセージのペイロード観点では，「隣接する CAN メッセージとペイロードの対象部が同一である挿入攻撃メッセージを挿入する場合」と，「隣接する CAN メッセージとペイロードの対象部が異なる挿入攻撃メッセージを挿入する場合」の 2 つに分割する．

次に，分割した部分集合と 3 つの特性の対応関係を示す．まず特性 1 は，図 5 の第 1 象限に該当する挿入攻撃（図 3 (a) のm_5）と第 2 象限に該当する挿入攻撃（図 3 (a) のm_8）の検知に有効な特性である．次に特性 2 は，図 5 の第 3 象

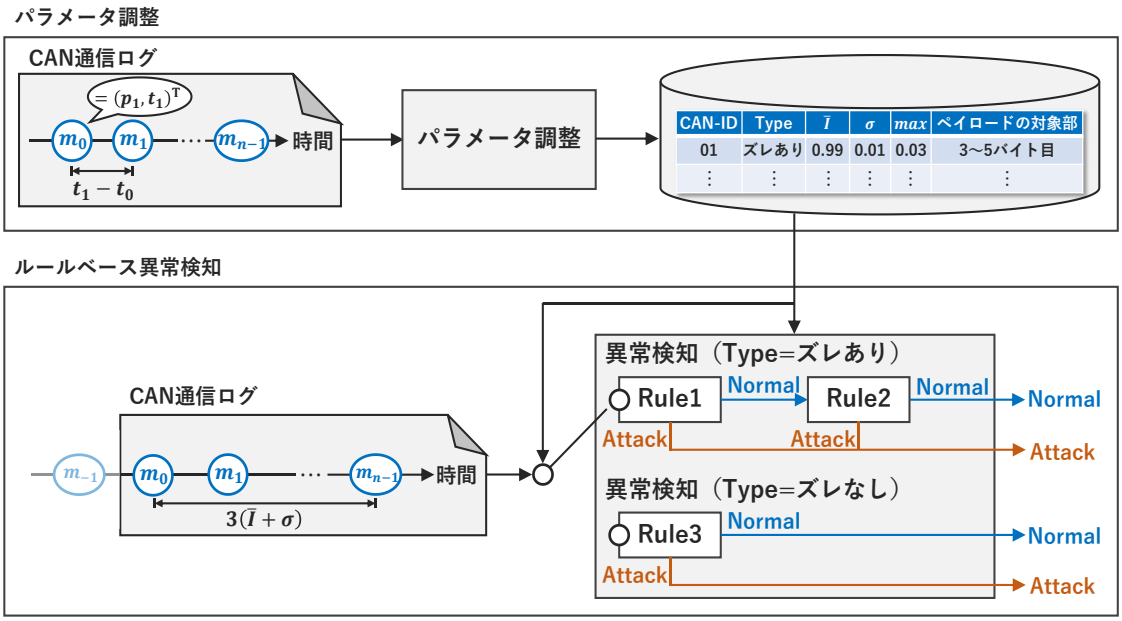


図 7　提案手法の全体像

限に該当する挿入攻撃（図 3 (b) のm_5）の検知に有効な特性である．そして特性 3 は，図 6 の第 1 象限に該当する挿入攻撃（図 3 (c) のm_9）と，第 2 象限に該当する挿入攻撃（図 3 (c) のm_{11}）と，第 3 象限に該当する挿入攻撃（図 3 (c) のm_7）の検知に有効な特性である．

図 5 と図 6 に示す通り，3 つの特性は第 4 象限に該当する挿入攻撃の検知に有効な特性ではない．つまり，3 つの特性を利用して図 5 と図 6 の第 4 象限に該当する挿入攻撃を検知することは不可能である．

一方，イベント送信付き周期型 CAN 通信において変化あり区間が発生することは少ない．また攻撃者が第 4 象限に該当する挿入攻撃を行うには，変化あり区間が発生するタイミングを予測しなければならない．しかし，変化あり区間はドライバーの操作に起因して発生する場合があり，その予測は攻撃者にとって容易ではない．つまり，第 4 象限に該当する挿入攻撃を実施することは攻撃者にとって困難性が高い．したがって，3 つの特性によって挿入攻撃のほとんどを漏れなく検知することが可能と考える．

4. 提案手法

3 章で述べた 3 つの特性をルール化し，そのルールを利用して異常検知を行う手法を提案する．

4.1 提案手法の全体像

後述する 3 つのルールにより異常検知を行う提案手法の全体像を図 7 に示す．提案手法はルールの利用に必要なパラメータ調整を行うフェーズと，ルールを用いて異常検知を行うフェーズの 2 つのフェーズからなる．パラメータ調整を行うフェーズでは，3 つのルールを利用する際に必要となるパラメータの調整を，パラメータ調整用の CAN 通信ログを用いて行う．詳細は 4.2 節で述べる．一方で異常検知を行うフェーズでは，Type に応じて利用するルールを選択し異常検知を行う．詳細は 4.3 節で述べる．

なお，本稿では 1 つの CAN-ID の CAN 通信を対象に異常検知を行う場合を例として説明する．検知対象の CAN-ID が複数ある場合は，本稿に記載されている提案手法を CAN-ID ごとに適用する．また，本稿ではある時間で得られたn個の CAN メッセージの時系列を$M = (m_0, m_1, \ldots, m_{n-1})$と表現する．また，$m_i$ $(0 \leq i < n)$のペイロードをp_i，送信時刻をt_iとし，$m_i = (p_i, t_i)^T$，$P = (p_0, p_1, \ldots, p_{n-1})$，$T = (t_0, t_1, \ldots, t_{n-1})$とする．

4.2 パラメータ調整

3 つの特性を利用したルールにより異常検知を行う際には，対象とする CAN-ID に対応する Type の情報やペイロードの対象部，送信間隔の平均値などのパラメータの調整が必要である．このパラメータ調整は，パラメータ調整用の CAN 通信ログに格納されている総数n個の CAN メッセージを用いて 4 つの手順で実施する．

手順 1 では，送信間隔の平均$\bar{I}$と標準偏差σを算出する．具体的には，$p_{i-2} = p_{i-1} = p_i$ $(2 \leq i < n)$を満たす$t_{i-1} - t_i$の平均$\bar{I}$と標準偏差σを求める．次に手順 2 では，$\bar{I}$からの送信間隔のズレの最大値maxを求める．具体的には，$p_{i-2} = p_{i-1} = p_i$ $(2 \leq i < n)$を満たす$\left|\bar{I} - (t_{i-1} - t_i)\right|$の最大値$max$を求める．そして手順 3 では Type を判定する．具体的には，$p_{i-2} \neq p_{i-1} = p$かつ$t_{i-1} - t_i \leq \bar{I}/2$ $(2 \leq i < n)$を満たす CAN メッセージが一つでも存在する場合は周期ズレなし型と判定し，それ以外を周期ズレあり型と判定する．最後に手順 4 では，ペイロードの対象部を特定する．具体的には，周期ズレあり型の場合はペイロードの対象部を全バイト位置とする．それに対して周期ズレなし型の場合は，$\bar{I} - max \leq t_{i-1} - t_{i-2}$かつ$\bar{I} - max \leq t_i - t_{i-1}$ $(2 \leq i < n)$を満

たすp_{i-1}とp_iで値変化が発生しているバイト位置をペイロードの対象部から除いていく．そして最後まで除かれなかったバイト位置をペイロードの対象部とする

以上の手順により，導出された Type と$\bar{I}$，σ，max，ペイロードの対象部の情報を CAN-ID と対応付けて記録する．

4.3 ルールベース異常検知

提案手法は，あるメッセージを起点に過去$3(\bar{I}+\sigma)$の時間内に送信されたn個の CAN メッセージの時系列Mを 1 つの検知対象とする．そして，その検知対象であるMの中に挿入攻撃メッセージが含まれているかどうかを判定する．$3(\bar{I}+\sigma)$の時間内としたのは，後述する Rule 3 を利用する際には少なくとも 3 つの周期メッセージが検知対象であるMの中に存在しなければならないためである．

異常検知を行う際はまず，検知対象の$P=(p_0,p_1,\dots,p_{n-1})$のうちペイロードの対象部のみに着目した$P'=(p'_0,p'_1,\dots,p'_{n-1})$を生成する．そしてこの$P'$と$T$を入力データとして利用する．次に検知対象である$M$の Type によって利用するルールを図 7 に示す通りに選択し，入力データと選択したルールを用いて異常検知を行う．

検知対象であるMの Type が周期ズレあり型の場合は特性 1 と特性 2 それぞれから構築した Rule 1 と Rule 2 を利用して異常検知を行う．

Rule 1 は「P'とTの中に，$p'_{i-1}=p'_i\ (1\le i<n)$，かつ$(t_i-t_{i-1})<(\bar{I}-max)$を満たす$p'_i$と$t_i$が存在する場合は Attack（異常）である．それ以外の場合は Normal（正常）である.」というルールである．Rule 1 による異常検知は Algorithm 1 により実現する．

Rule 2 は「P'とTの中に，$p'_j=p'_i\ (0\le i<n-2, i+2\le j<n)$，かつ$(\bar{I}-\sigma)\le(t_j-t_i)\le(\bar{I}+\sigma)$を満たす$p'_j$と$t_j$が存在する場合は Attack である．それ以外の場合は Normal である.」というルールである．Rule 2 による異常検知は Algorithm 2 により実現する．

検知対象であるMの Type が周期ズレなし型の場合は特性 3 から構築した Rule 3 を利用して異常検知を行う．

Rule 3 は「P'とTにおいて，$p'_{i-1}=p'_i\ (1\le i<n)$を満たす$t_i$が$(\bar{I}-\sigma)$以上かつ$(\bar{I}+\sigma)$以下の送信間隔で出現していなければ Attack である．また，特性 3 に従うと，$3(\bar{I}+\sigma)$の時間内で取得したP'とTの中には$p'_{i-1}=p'_i\ (1\le i<n)$を満たす周期メッセージが 2 つ以上存在する．したがって，挿入攻撃によりP'とTの中に$p'_{i-1}=p'_i\ (1\le i<n)$を満たす$t_i$が 2 つ以上存在しない場合も Attack である．そして，それ以外の場合は Normal である.」というルールである．Rule 3 による異常検知は Algorithm 3 により実現する．

Algorithm 1 Anomaly detection by Rule 1

```
procedure Rule1(P', T)
  for i ← 1 ... P'.length do
    diff ← T[i] − T[i − 1]
    if P'[i] = P'[i − 1] and diff < Ī − max then
      return Attack
    end if
  end for
  return Normal
end procedure
```

Algorithm 2 Anomaly detection by Rule 2

```
procedure Rule2(P', T)
  for i ← 1 ... P'.length − 2 do
    for j ← i + 2 ... P'.length do
      if P'[i] = P'[j] then
        diff ← T[j] − T[i]
        if diff ≥ Ī − σ and diff ≤ Ī + σ then
          return Attack
        end if
      end if
    end for
  end for
  return Normal
end procedure
```

Algorithm 3 Anomaly detection by Rule 3

```
procedure Rule3(P', T)
  Initialize memory: T_target ← []
  for i ← 1 ... P'.length do
    if P'[i − 1] = P'[i] then
      T_target.append(T[i])
    end if
  end for
  if T_target.length < 2 then
    return Attack
  end if
  for i ← 1 ... T_target.length do
    diff ← T_target[i + 1] − T_target[i]
    if diff < Ī − σ or diff > Ī + σ then
      return Attack
    end if
  end for
  return Normal
end procedure
```

5. 評価

本章では，実際の自動車から収集した CAN 通信ログを用いた提案手法の評価について述べる．

表 1　収集した CAN 通信ログの概要

メーカ	車種	パラメータ調整/学習用	評価用
A	X	約 4.8 時間	約 25.4 時間
B	Y	約 1.5 時間	約 1.5 時間

5.1 評価方法

評価に用いた CAN 通信ログの概要を表 1 に示す．CAN 通信ログは国内メーカ A の車種 X と国内メーカ B の車種

表 2　比較評価の結果（メーカ A の車種 X）

CAN-ID	Type	Koyama ら[14]の手法						提案手法					
		TP	FN	FP	TN	TPR	FPR	TP	FN	FP	TN	TPR	FPR
01	ズレなし	362	32	98	17192	91.88%	0.5668%	394	0	0	14757	100%	0%
02	ズレなし	361	33	0	90174	91.62%	0%	394	0	0	87681	100%	0%
03	ズレあり	59	15	68	90454	79.73%	0.0751%	70	4	0	88119	94.59%	0%
04	ズレあり	99	0	1	303030	100%	0.0003%	99	0	0	300643	100%	0%
05	ズレあり	0	0	0	88092	-	0%	0	0	3	85734	-	0.0035%
06	ズレあり	655	104	3	88006	86.30%	0.0034%	741	18	0	85393	97.63%	0%
07	ズレあり	1203	113	0	89384	91.41%	0%	1298	18	0	86973	98.63%	0%
08	ズレあり	80	24	25	8379	76.92%	0.2975%	64	40	0	5853	61.54%	0%
09	ズレあり	0	0	86	44292	-	0.1938%	0	0	0	42018	-	0%
10	ズレあり	0	0	0	7696	0%	0%	0	22	0	5349	0	0%
11	ズレあり	24	0	16	304294	100%	0.0053%	21	3	0	301919	87.50%	0%
12	ズレあり	270	0	0	90081	100%	0%	270	0	0	87654	100%	0%
13	ズレあり	396	0	67	89916	100%	0.0745%	375	21	0	87488	94.70%	0%
14	ズレあり	777	3	71	89948	99.62%	0.0789%	755	25	0	87424	96.79%	0%
15	ズレあり	99	0	0	90167	100%	0%	99	0	0	87779	100%	0%
16	ズレあり	0	0	35	304752	-	0.0115%	0	0	0	302429	-	0%
Total		4385	324	470	1795857	93.12%	0.0262%	4580	129	3	1757213	97.26%	0.0002%

Y からパラメータ調整/学習用と評価用に分けて収集した．メーカ A の車種 X のパラメータ調整/学習用の CAN 通信ログは，3.1 節で述べた「挿入攻撃を実施せずに収集した CAN 通信ログ」と同一である．また，メーカ A の車種 X の評価用の CAN 通信ログは，3.1 節で述べた「挿入攻撃を実施しつつ収集した CAN 通信ログ」と同一である．一方でメーカ B の車種 Y のパラメータ調整/学習用の CAN 通信ログと評価用の CAN 通信ログは，両方とも 3.1 節に示した方法で挿入攻撃を実施せずに収集した．

本評価では，提案手法と Koyama ら[14]の手法との比較評価を行った．評価に先立ち，表 1 のパラメータ調整/学習用の CAN 通信ログを用いて提案手法のパラメータ調整と Koyama ら[14]の手法の学習を車種ごと CAN-ID ごとに行った．その後，表 1 の評価用 CAN 通信ログのうちイベント送信付き周期型 CAN 通信ログのみを用いて，提案手法と Koyama ら[14]の手法それぞれで異常検知を行った．

そして，True Positive (TP) と False Negative (FN)，FP，True Negative (TN)，TPR，FPR の 6 つの評価指標を用いて提案手法と Koyama ら[14]の手法を比較評価した．なお TP は一度でも異常と判定された挿入攻撃メッセージ数であり，FN は全挿入攻撃メッセージから TP を減算した数である．また，FP は挿入攻撃メッセージを含まない検知対象を異常と判定した数であり，TN は挿入攻撃メッセージが含まれない検知対象の数から FP を減算した数である．そして TPR と FPR は式 (1) と式 (2) の通りである．

$$\mathrm{TPR}[\%] = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \times 100 \qquad (1)$$

$$\mathrm{FPR}[\%] = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \times 100 \qquad (2)$$

また，提案手法が Koyama ら[14]の手法より低い FPR での異常検知が可能かどうかを確認するために，式 (3) で定義

表 3　比較評価の結果（メーカ B の車種 Y）

CAN-ID	Type	Koyama ら[14]の手法			提案手法		
		FP	TN	FPR	FP	TN	FPR
01	ズレなし	3	271276	0.0011%	0	271174	0%
02	ズレあり	11	54391	0.0202%	4	54353	0.0074%
03	ズレあり	3	54448	0.0055%	0	54406	0%
04	ズレあり	1	54547	0.0018%	0	54502	0%
05	ズレあり	23	90525	0.0254%	153	90350	0.1691%
06	ズレあり	0	54357	0%	0	54312	0%
07	ズレあり	190	54198	0.3493%	27	54316	0.0497%
08	ズレなし	97	54258	0.1784%	0	54322	0%
09	ズレあり	15	55308	0.0271%	2	55276	0.0036%
10	ズレなし	9	54260	0.0166%	0	54224	0%
Total		352	797595	0.0441%	186	797235	0.0233%

する FPR の低減量も評価指標として用いた．

$$\text{FPR の低減量} = \frac{\text{提案手法の FPR}}{\text{Koyama ら[14]の手法の FPR}} \qquad (3)$$

5.2 結果

比較評価の結果を表 2 と表 3 に示す．表 2 はメーカ A の車種 X から収集した評価用の CAN 通信ログにそれぞれの手法を適用した際の結果である．一方で，表 3 はメーカ B の車種 Y から収集した評価用の CAN 通信ログにそれぞれの手法を適用した際の結果である．

Result 1: 表 2 と表 3 に示す通り，提案手法の結果のうちメーカ A 車種 X の CAN-ID=05 とメーカ B 車種 Y の CAN-ID=02, 07, 09 の結果に FP が存在した．これは 3.2.2 項で述べた特性 2 に反するイベントメッセージを誤って異常と判定したためであった．

Result 2: 表 3 に示す通り，提案手法の結果のうちメーカ B の車種 Y の CAN-ID=05 の結果に比較的多くの FP が存在した．この原因は，隣接した直前の CAN メッセージとペイロードの対象部が同一である正常な CAN メッセージが周期間隔よりも短い送信間隔で送信されていたためであっ

た．これは Rule 1 で異常と判定される特性であり，この特性を持つ正常な CAN メッセージを Rule 1 で誤って Attack と判定したため FP が発生した．

Result 3: 提案手法は，メーカ A の車種 X の結果において約 2.7%の挿入攻撃メッセージを見逃しており，特に CAN-ID=08 における挿入攻撃メッセージの見逃しが多かった．この原因は図 5 と図 6 の第 4 象限に該当する挿入攻撃メッセージを見逃したためであった．特に CAN-ID=08 の CAN 通信には変化あり区間が多く，半分近くの挿入攻撃メッセージが変化あり区間に挿入されていたため見逃しが多かった．

Result 4: メーカ A の車種 X から収集した評価用の CAN 通信ログを用いて提案手法と Koyama ら[14]の手法を比較評価した結果，提案手法の FPR は約 0.0002%であり，FPR の低減量は約$1/154$であった．また提案手法の TPR は約 97.26%であり, Koyama ら[14]の手法より約 4.14%高かった．

5.3 考察

Result 1 で述べた通り, 提案手法では特性 2 に反する CAN メッセージを誤って異常と判定したことによる FP が発生していた．その FP 数は 3.2.2 項で考察した通り，メーカ A 車種 X の結果では比較的少ない数に抑えられていたと考える．一方でメーカ B 車種 Y の結果では，特性 2 に反する CAN メッセージを誤って異常と判定したことによる FP が比較的多く発生していたと考える．よって, Rule2 の改善や新たなルールの創出，他の手法との組合せなどの提案手法の改良が必要と考える．

Result 2 で述べた通り，Rule 1 が正常な CAN メッセージを誤って異常と判定する特性を持つ CAN 通信がメーカ B の車種 Y において発生していた．このことから提案手法の 3 つの Rule が必ずしもすべての車種において成立するとは限らないことが示唆された．

Result 3 で述べた通り，提案手法は図 5 と図 6 の第 4 象限に該当する挿入攻撃メッセージを見逃していた．また，一部の CAN-ID では図 5 と図 6 の第 4 象限に該当する挿入攻撃メッセージの見逃しが多く発生していた. したがって，TPR をより高めるためには図 5 と図 6 の第 4 象限に該当する挿入攻撃を検知可能なルールの考案や，他の手法との組み合わせなどの手法の改良が必要と考える．

Result 4 で述べた通り，提案手法は Koyama ら[14]の手法と比較して FPR を約$1/154$に低減しつつ約 4.14%高い TPR での異常検知を実現した．よって提案手法は，イベント送信付き周期型 CAN 通信に対しての挿入攻撃の検知に有効な手法だと考える．

6. まとめ

本研究では，イベント送信付き周期型 CAN 通信に対しての挿入攻撃を検知することが可能なルールベース異常検知手法を提案した．そして，メーカの異なる 2 車種の自動車に対して挿入攻撃を実施しつつ収集した CAN 通信ログを用いた評価を行った．その評価では，イベント送信付き周期型 CAN 通信を対象とした先行研究[14]の手法と提案手法の比較評価を行った．その結果，提案手法は TPR = 97.26%（先行研究[14]と比較して約 4.14%向上），FPR = 0.0002%（先行研究[14]と比較して FPR を約$1/154$に低減）を実現可能であることを示した．

今後はルールの改良や新たなルールの創出，他の手法との組み合わせるにより，より一層の FPR の低減と TPR の向上に取り組んでいく．また，より多くのメーカのより多くの車種を対象に提案手法の汎用性評価を実施していく．

参考文献

[1] ISO 11898-2, “Road vehicles - Controller area network (CAN) - Part2: High-speed medium access unit,” 2016.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” In *Proc. 20th USENIX conference on Security*, 2011, pp.1-16.

[3] I. Rouf, R. Miller, H.Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,” In *Proc. 19th USENIX Security Symposium*, pp.1-16, 2010.

[4] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” In *Proc black hat USA 2015,* 2015, pp.1-91.

[5] C. Young, J. Zambreno, H. Olufowobi, and G Bloom, “Survey of Automotive Controller Area Network Intrusion Detection Systems,” In *Proc. IEEE Design & Test*, 2019, Vol. 36, No. 6, pp.48-55.

[6] G. Dupont, J. D. Hartog, S. Etalle, and A. Lekidis, “A Survey of Network Intrusion Detection Systems for Controller Area Network,” In *Proc. 2019 IEEE ICVES*, 2019, pp.1-6.

[7] M. Gmiden, M. H. Gmiden, and H. Trabelsi, “An Intrusion Detection Method for Securing In-Vehicle CAN bus,” In *Proc. 17th STA*, 2017, pp.176-180.

[8] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, “Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks,” in *Proc. CISRC 2017*, 2017, pp.1-4.

[9] S. Otsuka and T. Ishigooka, “CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems Overview of In-Vehicle Networks,” In *SAE Technicol paper*, 2014, pp1-11.

[10] A. Taylor, N. Japkowicz, and S. Leblanc, “Frequency-Based Anomaly Detection for the Automotive CAN bus,” In *Proc. 2015 WCICSS*, 2015, pp.45-49.

[11] A. Taylor, S. Leblanc, and N. Japkowicz, “Anomaly Detection in Automotive Control Network Data with Long Shor-Term Memory,” In *Proc. 2016 DSAA*, 2016, pp.130-139.

[12] 福田 國統, 磯山 芳一, 濱田 芳博, 畑 洋一, “CAN 通信における汎用的な攻撃検出を目的とした時系列データ解析,” 情報処理学会 CSS2018, 2018, pp.1-8.

[13] 矢嶋 純, 長谷部 高行, 大久保 隆夫, “値の遷移に着目した車載向け攻撃検知のためのデータ関連性分析手法,” 電子情報通信学会 SICS2019, 2019, pp.1-7.

[14] T. Koyama, T. Shibahara, K. Hasegawa, Y. Okano, M. Tanaka, and Y. Oshima, “Anomaly Detection for Mixed Transmission CAN Messages Using Quantized Intervals and Absolute Difference of Payloads,” In *Proc. ACM AutoSec 2019*, 2019, pp.19-24.