CAN のイベントメッセージに対する侵入検知手法の提案

濱田　芳博[†1]　吉田 圭吾[†1]　足立　直樹[†2]　上口 翔吾[†2]
上田　浩史[†2]　宮下 之宏[†2]　礒山　芳一[†1]　畑　　洋一[†1]

概要：近年の車両は車載制御ネットワークにより接続された 70～100 台の Electronic Control Unit(ECU)により制御されると共に，車両外の様々なサービスとネットワークを介して制御データを共有し利便性を向上させている．一方で車両外から車載ネットワークへ悪意のあるメッセージを注入することでこれらの利便性を阻害するサイバー攻撃が問題視されており，対策が急がれている．侵入検知は監視対象がサイバー攻撃を受けたことを検知する技術であり，サイバー攻撃への対策を開始するための重要な情報を与える．監視対象が車載ネットワークの場合，侵入検知アルゴリズムとしては本ネットワークで周期的に送信されるメッセージの周期性の逸脱を検出する方法が知られている．しかし車載ネットワークでは周期的に送信されないイベントメッセージも存在し，車両へのサイバー攻撃の事例ではこの様なメッセージも攻撃対象となる．しかし周期的に送信されるメッセージを監視する侵入検知アルゴリズムでは，イベントメッセージに対して行われた攻撃の検知を行うことができない．そこで本論では，イベントメッセージに対する侵入検知アルゴリズムを提案する．

キーワード：侵入検知，車載ネットワーク，イベントメッセージ，CAN

Intrusion Detection for Acyclic Messages in In-Vehicle Network: A Proposal

Yoshihiro Hamada[†1]　Keigo Yoshida[†1]　Naoki Adachi[†2]　Shyogo Kamiguchi[†2]
Hiroshi Ueda[†2]　Yukihiro Miyashita[†2]　Yoshikazu Isoyama[†1]　Yoichi Hata[†1]

Abstract: The automotive industry intends to create new services that involve sharing control information of a vehicle via a wide area network. However, some incidents of cyber-attacks to a vehicle show that a connection to outer of a vehicle is abused for cyber-attacks. Therefore, improving security measures of a vehicle are urgent to realize new services. To realize security measures of a vehicle, it is important to detect cyber-attacks at first. And, the intrusion detection system (IDS) is known as a technique of detecting cyber-attacks. For the IDS algorithm of the in-vehicle network, the monitoring communication cycle period of cyclic messages is known as the popular method. On the other hand, there are also acyclic messages in the in-vehicle network, and these messages would be an important target to be success cyber-attacks. However, it is difficult to detect cyber-attacks to acyclic messages using the IDS algorithm for cyclic messages. Therefore, in this paper, we will propose the IDS algorithm for acyclic messages.

Keywords: Intrusion Detection System, In-vehicle network, Acyclic messages, CAN

1. はじめに

近年の車両は，車載制御ネットワークにより接続された 70～100 台の Electronic Control Unit(ECU)と呼ばれる組み込みコントローラにより制御されると共に，車両外の様々なサービスとネットワークを介して制御データを共有することで，車両の安全性や利便性を向上させている．一方でこの様な車両が持つ外部との通信機構を悪用して，車両を外部から不正に制御するサイバー攻撃の可能性が示されており，このためのセキュリティ対策が急がれている [1]. サイバー攻撃に対しては適切なセキュリティ対策を実施するために，監視対象が攻撃を受けたことを検知する必要があり，この手段として侵入検知（Intrusion Detection System: IDS）が知られている．車載ネットワークでの侵入検知方式の一つに，均一な時間間隔で繰り返し送信されるメッセージ（周期メッセージ）に対してなりすましメッセージを注入するサイバー攻撃を効果的に検知可能なメッセージ通信間隔の監視方式が知られている[2][3][4]．しかし車載ネットワークでは，制御状態の不定期な変更を通知するために送信時間間隔が不均一となるメッセージ（イベントメッセージ）も使用される．車両へのサイバー攻撃ではこの様なイベントメッセージも重要な攻撃対象となるが，従来の周期メッセージに対する監視方式ではこの検知が困難である．そこで本論では，イベントメッセージの監視を行う２種類の方

†1 住友電気工業株式会社
SUMITOMO ELECTRIC INDUSTRIES, LTD.
†2 オートネットワーク技術研究所株式会社
Autonetworks Technologies, Ltd.

式について提案を行う．

1.1 構成

本節以降の構成を示す．第 2 節では CAN プロトコルとセキュリティ脅威について説明する．第 3 節では車載ネットワークのセキュリティ技術を示し，第 4 節ではイベントメッセージを監視する場合の従来の車載侵入検知システムの課題を示す．第 5 節で提案手法を示し，第 6 節にて本提案手法の評価結果を示す．第 7 節にはまとめと今後の展開を示す．

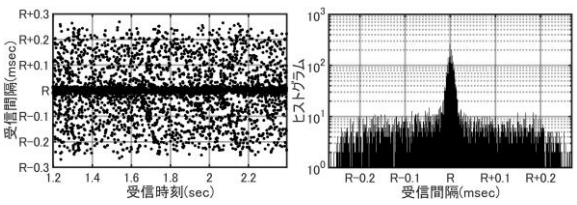
2. CAN プロトコルとセキュリティ脅威

2.1 CAN の特徴

CAN プロトコルと CAN-FD プロトコルの 2 つがある．CAN プロトコルは ISO11898-1(2003)で標準化され，CAN-FD プロトコルは同標準を改訂する形で ISO11898-1(2015)にて標準化された[5][6]．本プロトコルでは，バス型のトポロジ上の複数のノード（ECU）の内，通信調停により送信権を得たノードが最大 8 バイト（CAN）または 64 バイト（CAN-FD）のペイロードをブロードキャスト送信することで，制御システム用途での低遅延なメッセージの通信を実現している．

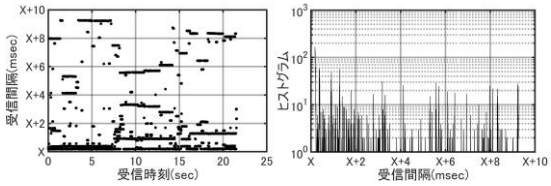
2.2 メッセージの通信パタン

CAN プロトコルを適用した車載ネットワークでのメッセージの通信パタンは，大きく 2 種類に分類できる．一つは均一な時間間隔で繰り返しメッセージが送信される通信パタンであり，速度，エンジン回転数やアクセル開度といった一定時間間隔で変化する制御データの通信に用いられる．本論ではこの様な通信パタンを持つメッセージを「周期メッセージ」と呼ぶ．図 1 に周期メッセージの受信間隔を a)時間軸と b)ヒストグラムにより示す．周期メッセージでは受信間隔は時刻 R を中心に分布しており，その分布は b)の様にガウス状となる．もう一つの通信パタンは不均一な時間間隔でメッセージが送信され，ドアの開錠・施錠，ギアのシフトや方向指示器の操作，といった不定期に変化する制御データの通信に用いられる．本論ではこの様な通信パタンを持つメッセージを「イベントメッセージ」と呼ぶ． 図 2 に本メッセージの受信間隔を a)時間軸と b)ヒストグラムにより示す．イベントメッセージでは周期メッセージと比較して受信間隔が広い時間範囲に一様に分布する．



a)時間軸　　b)ヒストグラム

図 1. 周期メッセージの受信間隔



a)時間軸　　b)ヒストグラム

図 2. イベントメッセージの受信間隔

2.3 セキュリティに対する脅威

Koscher らは CAN プロトコルについて次に示す 3 つの脆弱性を指摘している[7]. (1)ネットワーク上の制御情報を容易に解析可能，(2)なりすましメッセージを容易に挿入可能，(3)Denial of Service(DoS)攻撃に弱い．なりすましメッセージの挿入や DoS 攻撃は，図 3 に示す様に，CAN バスに接続される攻撃 ECU を介して行われる．これは，正常な ECU のファームウェアを改ざんしたものか，不正な ECU を接続したものである．

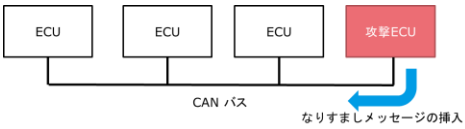


図 3. 攻撃 ECU によるなりすましメッセージの挿入

3. 車載ネットワークのセキュリティ対策

3.1 従来技術

車載ネットワークでのセキュリティに関する研究は以下の 2 つに分類できる．

(1) セキュア通信
　ネットワークプロトコルでのセキュリティ対策を行う．

(2) 侵入検知システム
　ネットワークプロトコル上で動作し，アプリケーションやネットワークでの疑わしい動きを検出する．

3.2 侵入検知システム

3.2.1 技術分類

侵入検知システムは，ネットワーク型とホスト型の 2 つの技術に分類される．ホスト型は一つのノードに設置されるため，システムや接続されたネットワークセグメントの監視を行うことができる．これに対し，ネットワーク型は全てのネットワークセグメントが監視できる場所に設置される．一般的に，車両では複数のネットワークセグメントによって 70 を越える ECU が接続される．本論では，ネットワーク型侵入検知システムを採用することで，多数の ECU を少ない侵入検知システムにより監視する．

3.2.2 検知方式

侵入検知方式にはシグネチャー型とアノマリ型の 2 種類がある．これらは監視対象の疑わしい振る舞いを検知することで侵入を検知する．シグネチャー型は監視対象の誤った使用例と一致するものを検知する．この方式では検知条

件として，既知のサイバー攻撃による監視対象の例外的な使用例を定義する．アノマリ型は，監視対象の振る舞いが正常時の振る舞いから逸脱するものを検知する．この方式では，検知条件として監視対象の正常時の振る舞いを定義する．

一般的にアノマリ型はシグネチャー型と比較して誤検知率が高いが，未知のサイバー攻撃の検知が可能である．本論ではアノマリ型の検知方式を採用する．

3.2.3 従来の車載侵入検知方式

車載ネットワーク用の侵入検知方式の研究には，未知のサイバー攻撃を検知するために，以下に示す多くのアノマリ型の検知方式がある．

Larson らは，仕様ベースの侵入検知を CANopen2.1 に適用した[8]．この方式では，CANopen2.1 プロトコルで定義されるルールから逸脱した場合に検知を行う．

Otsuka らは周期メッセージについて，通信頻度の監視を行う侵入検知を提案した[3]．周期メッセージの受信間隔はプロトコルによって揺らぐため，この方式ではメッセージ毎に最大遅延時間を学習して，この時間内で受信されるメッセージ数を計数する．他の研究に複数の周期メッセージの通信頻度を監視する方式がある[13]．

周期メッセージの通信間隔を監視する研究に，次に示す Müter らの方式に加え，メッセージ受信間隔のゆらぎを確率密度関数により学習して監視を行うものがある[4]．

Müter らは，エントロピーベースの検知方式を提案した[2]．この方式は周期メッセージの受信間隔や，メッセージに含まれる制御データのエントロピーを式(1)により算出し，監視を行う．数式(1)において，C_XはデータセットXのクラスであり，$p(x)$はXに含まれるxの発生確率である．このため，この方式では監視対象の発生確率を学習する必要がある．

$$H(X) = \sum_{x \in C_X} p(x) log \frac{1}{p(x)} \qquad (1)$$

Malkovitz らは，メッセージに含まれる，制御データの値域を監視する方式の提案を行った[9]．ここで用いられる値域は，監視対象の制御データの最大ビット長によるものでは無く，車両を走行させた場合の実効的な可変範囲である．

Wasicek らは Semantic Based の検知方式を提案した[10]．この方式では，車両物理モデル（例えばエンジン回転数に対するトルクの特性）に基づいて，車両内や車両外（路面状況等）から得た情報より監視対象の制御データの値を算出し監視を行う．

筆者らは速度等の連続データを車載ネットワークから得られる相関データを用いて監視する方式を提案した[11]．

鶴見らはドアロックの ON/OFF の様な状態を示すデータをフラグデータと定義し，本データを監視する方式を提案した[12]．監視対象のフラグデータと他のフラグデータの状態遷移を学習し，学習済みの遷移から逸脱した場合に異常を検知する．

4. イベントメッセージ監視の課題

4.1 攻撃モデル

イベントメッセージに対する攻撃モデルを図 4 に示す．共有バスモデルと示した本モデルでは，攻撃者が攻撃 ECU を介して，攻撃対象とするイベントメッセージになりすましメッセージの挿入を行う．攻撃者がなりすましメッセージの挿入を行う際，なりすましメッセージの送信間隔が均一な攻撃を「周期攻撃」，不均一な攻撃を「不定期攻撃」と定義する．

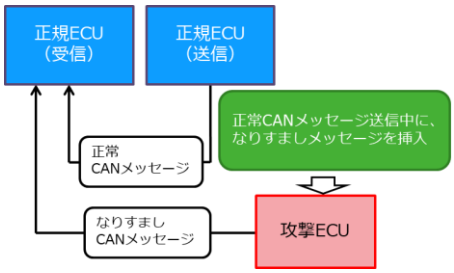


図 4. 共有バスモデル

4.2 監視モデル

図 5 に本論で前提とする車載ネットワークでの侵入検知モデルを示す．本モデルでは，監視対象とする CAN バスのトラフィックを観測可能な ECU 上で集中監視を行う．検知結果を基にしたセキュリティ対策は次の 2 種類が考えられる．一つは検知結果を基に疑わしい挙動の一時的な抑制を行う「即時応答」である．もう一つは他の情報と照合して，疑わしい挙動の根本原因を特定した後に根本対策を行う「遅延応答」である．いずれの応答においても，侵入検知アルゴリズムによる攻撃の見逃しや，攻撃の過検知等の誤検知の低減は重要な要件である．

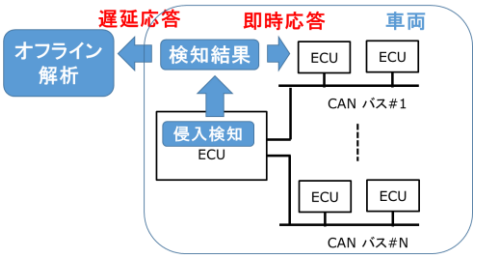


図 5. 侵入検知と応答モデル

4.3 課題

従来の車載侵入検知方式によるイベントメッセージを監視する場合の課題を，「ペイロード監視」と「周期監視」の 2 種類に分類して検討する．「ペイロード監視」にはイベントメッセージに含まれる制御データを監視する方法を分類し，「周期監視」にはイベントメッセージの受信間隔や受信頻度を監視する方法を分類した．また本論では，イベントメッセージにより伝送されるデータは，ドアの開錠・施錠，ギアのシフトや方向指示器の操作，といった複数の制御状態を「センサデータ」よりは小さい値域の離散値で示す「状

態データ」と定義した．ここで「センサデータ」は，速度やエンジン回転数等の時系列において連続的に値が変化し，広い値域で示される離散値と定義する．

4.3.1 ペイロード監視の課題

表 1 にペイロード監視によるイベントメッセージに対する攻撃検知可能性を示す.「方式」には各方式についての巻末の参考文献番号を示す.「監視対象」には各方式が監視する制御データの特性を示し,「攻撃検知」には各方式によりイベントメッセージに対する攻撃検知可能性を３つの記号を用いてランク付けする.「○」は可能,「△」は改善により可能そして「×」は困難を意味する．時系列での制御データの値の変化を監視する[2]の方式では攻撃の検知は困難とした．この方式では直前の状態から次の状態へ遷移する際の制御データの差異を監視するが，状態データの値域は狭く，攻撃により生じた直前の制御データとの差異を通常時と区別することが難しいためである．制御データの値の変化の範囲を監視する[9]の方式についても，攻撃の検知は困難とした．この方式では制御データが通常時の可変範囲から外れる場合を異常とするが，状態データの場合は攻撃によって他の状態を示す値が指定されるため，値域外の値が指定されることは無く，通常時との区別が難しいためである．監視モデルによる推定値を比較する方法では，[10][11] [12]の方法は改善により可能とした. [10][11]の方法はセンサデータを監視対象とするため，モデルの学習を状態データに対して適合させる必要がある. [12]の方式は, 監視対象の状態データと他の状態データの状態遷移を学習し状態遷移が逸脱した場合を異常と判定する. この方式では, 監視対象と他の状態データの間に相関関係が成立しない場合，監視のために有用な状態遷移の抽出が難しい．状態遷移を学習するための制御データの組み合わせを発見する方法について検討が必要である．

表 1．ペイロード監視での攻撃の検知

方式	監視対象	攻撃検知
[2]	時系列での値の変化	×
[9]	値の変化の範囲	×
[10][11][12]	監視モデルによる推定値との比較	△

4.3.2 周期監視の課題

表 2 に「周期監視」によるイベントメッセージに対する攻撃検知可否を示す.「方式」,「監視対象」,「攻撃検知」には 4.3.1 と同じ内容を示す.「スレッショルド決定方法」では監視対象で異常が発生したと判断するためのスレッショルドの決定方法を示す. 受信間隔を監視する[2][4]の方式では検知が困難とした．これらの方式では判断のためのスレッショルドとして通常時の受信間隔を決定する必要があるが，イベントメッセージの受信間隔は図 2 b)に示す様に時間に対し一様に分布するためこの定義が不可能なためである．受信頻度を監視する[3]の方式も検知が困難とした．この方式は，監視対象とするメッセージの最大遅延時間までに，受信するメッセージ数が 2 つ以上となる場合を異常とする．このため，受信頻度が 2 つ以上になるイベントメッセージを，この方式により監視することは難しい．受信頻度を監視する[13]の方式は改善により検知が可能とした．この方式は CAN メッセージの受信頻度の外れ値を監視する方式である．このためスレッショルドには受信頻度の最大値が設定される．イベントメッセージの受信頻度は時系列で大きく変動するため，この方式では正常メッセージの受信頻度が低い時に攻撃を受けると，挿入される攻撃メッセージの送信頻度によっては検知が困難になる．

表 2．周期監視での攻撃の検知

方式	監視対象	スレッショルド決定方法	攻撃検知
[2] [4]	受信間隔	トラフィックから通常時の受信間隔を決定	×
[3]	受信頻度	トラフィックからメッセージの最大遅延時間を決定	×
[13]	受信頻度	トラフィックから通常時に受信する複数メッセージの受信頻度を決定	△

5. 提案手法

メッセージ中のペイロードに含まれる状態データ毎に監視するペイロード監視方式と，メッセージ毎に監視するための周期監視方式の２つの方式を提案する．ペイロード監視方式は状態データ毎の監視を行うため，一つのメッセージに複数の状態データが含まれる場合には，複数の監視モデルを作成する必要がある. メモリや CPU の速度などの計算リソースの制限により，全ての状態データの監視が難しい場合には，監視モデルに応じて 2 つの監視方式の何れを単独で使用するか，あるいは 2 つの方式を併用するかを決定する．

5.1 節にペイロード監視方式を示す. 本方式は，筆者達がセンサデータを監視するために提案を行った CDEC を拡張した [11]. 監視対象となる状態データを，当該データに対する相関データ群から車両データモデルを介して推定し，両者の値が一致しない場合を異常として検知する．センサデータ監視のためには車両データモデルに Least Absolute Shrinkage and Selection Operator (LASSO)や回帰木を用いたが, これらは状態データを取り扱うことが困難であるため, 提案方式では，データモデルに決定木を用いた．

5.2 節に周期監視方式を示す. 本方式では, イベントメッセージの受信間隔の監視を行う．イベントメッセージの受信間隔は不均一であるため，現在のイベントメッセージの受信間隔の不規則性を，過去の受信間隔との自己相関係数を算出して評価する．算出した自己相関係数が閾値を超え

た場合を異常として検知する．

5.1 ペイロード監視方式

図 6 に本提案方式のアプリケーションモデルを示す．本アプリケーションが監視対象状態データを含むメッセージを受信した場合，「推定器」は以前に受信された相関制御データ群から，5.1.1 節に示す方法で事前に学習した車両データモデルを介して監視対象状態データの推定値を算出する．次に「評価器」が監視対象状態データの現在値と推定値を比較し，これらが一致しない場合，現在の状態データを異常と判定する．「報告器」は現在の状態データが異常の場合，状況の記録やセキュリティ対策を実施する他のシステムに通知を行う．「分割器」は監視対象状態データや相関データ群を含むメッセージが受信される度に，制御データをメッセージから抽出して記憶する．

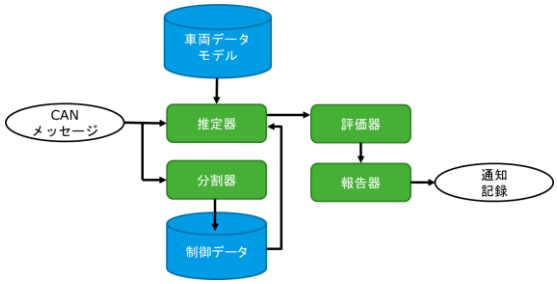


図 6．状態データを監視する場合の
CDEC アプリケーションモデル

5.1.1 車両データモデルと事前学習

車両データモデルには図 7 に示す決定木を用いる．決定木は一つの根と 2 つの葉を持つ 2 分木を重ね合わせて構成される．2 分木では，「根」で相関制御データの現在値と閾値が比較してどちらの「葉」を選択するか判定した後に，「葉」に割り当てられた状態データを推定値として選択する．決定木が複数の 2 分木で構成される場合には，2 分木が連結される「葉」は別の 2 分木の「根」となる．「根」で使用される相関制御データと閾値及び「葉」に割り当てる状態データの値は，Classification And Regression Tree（CART）法を用いて「相関制御データ」から決定される[14]．「相関制御データ」は監視対象状態データに対して相関関係のある制御データであり，5.1.2 節に示す様に抽出する．

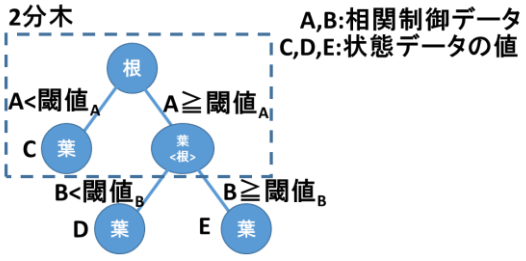


図 7．2 分木による決定木

5.1.2 相関制御データの抽出

監視対象状態データと相関関係のある制御データは，両者の相互相関係数を数式(2)により算出し，この結果が相関関係を示す場合に抽出する．rは相互相関係数であり，xとy，μ_x とμ_yは各々，監視対象状態データと他の制御データとそれぞれの平均であり，nはサンプル数を示す．相互相関係数は 0～±1.0 の範囲で変化し，値が 1.0 または-1.0 に近い程 2 つのデータの相関関係が強い．一般的に相互相関係数が 0.4 以上，-0.4 以下で相互に相関関係があると言われる．本論でもこれらの値を閾値として正，負の制御データを相関制御データとして抽出する．

監視対象状態データと他の制御データが異なるメッセージに含まれる場合は，それぞれのデータのサンプリング間隔が異なるため，相互相関係数の算出前に図 8 に示す様に，監視対象状態データのサンプリング間隔で他の制御データをリサンプリングする．

$$r = \frac{\sum_{i=1}^{n}(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum_{i=1}^{n}(x_i - \mu_x)^2}\sqrt{\sum_{i=1}^{n}(y_i - \mu_y)^2}} \qquad (2)$$

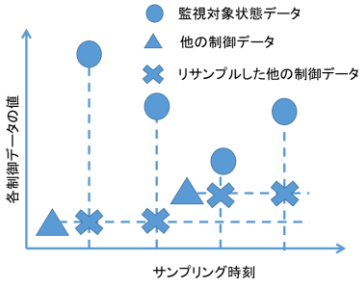


図 8．監視対象状態データと他の制御データ

5.2 周期監視方式

図 9 に本提案方式のアプリケーションモデルを示す．本アプリケーションが監視対象とするイベントメッセージを受信した場合，「受信間隔測定器」が直前に受信したメッセージからの時間間隔を算出し，受信時刻列として記憶する．次に「自己相関器」が 5.2.1 節に示す様に過去に受信した受信間隔列と，現在の受信間隔列の相関係数を算出する．この後「評価器」により算出された自己相関係数が，5.2.2 節に示す方法で事前に決定されたスレッショルドと比較される．受信間隔の自己相関係数がスレッショルドを超える場合には，報告器により状況の記録やセキュリティ対策を実施する他のシステムに通知される．

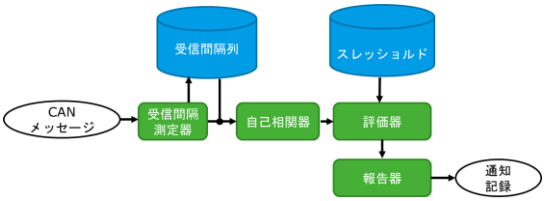


図 9．イベントメッセージを監視する場合の
周期監視アプリケーションモデル

5.2.1 受信間隔列の自己相関係数

イベントメッセージの受信間隔の自己相関係数は，図 10 に示す様に「ウィンドウ」に記憶された直前に受信されたメッセージからの受信間隔（D1～D6）を「過去の受信間

隔列」と「現在の受信間隔列」に分け，これらの自己相関係数を数式(1)により算出する．rは自己相関係数であり，xとy，μ_x とμ_yは各々現在と過去の受信間隔列の受信間隔とそれぞれの平均であり，nはサンプル数を示す．自己相関係数は 0～±1.0 の範囲で変化し，値が 1.0 または-1.0 に近い程現在と過去の受信間隔列の相関関係が強くなる．この計算に用いる受信間隔，xとyは，数式(3)により事前に変換する．

$$受信間隔の変換 = 受信間隔 \times (-1)^n$$
$$計算毎に更新：n = n + 1, \quad 初期値：n = 0 \quad (3)$$

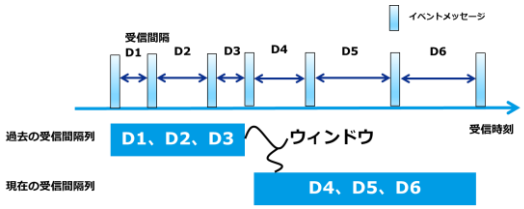


図 10．イベントメッセージ受信間隔の自己相関係数算出

5.2.2 スレッショルド

受信間隔の自己相関係数の正の値の最大値と，負の値の最小値の絶対値の内，大きいものをスレッショルドとして用いる．正の自己相関係数が本スレッショルドを超える，あるいは負の自己相関係数が本スレッショルドを下回る場合を異常と判定する．本スレッショルドは，攻撃メッセージが含まれない正常時のトラフィックから取得する

6. 評価

2 つの提案手法（ペイロード監視方式，周期監視方式）の検知率を，6.1 節に示すトラフィックデータを用いて，6.2 節に示す基準により評価を行った．比較対象には，イベントメッセージの監視に一般的に用いられる，6.3 節に示す頻度監視手法を用いた．検知率の評価に先立ち， 2 つの提案方式と比較方式について，6.4 節に示す様にパラメータの調整を行った．6.5 節に検知率の評価結果を示す．

6.1 評価用トラフィックデータ

検知率の評価に用いるトラフィックデータは，図 11 に示す環境を用いて，試験車両で取得したトラフィックデータに疑似的な攻撃メッセージを挿入して作成した．表 3 に攻撃ノードからの攻撃メッセージの挿入条件を，2 つの攻撃形態（周期攻撃，不定期攻撃）について示す．「周期攻撃間隔」には攻撃ノードからの攻撃メッセージの送信間隔を示し，「不定期攻撃間隔」には，攻撃ノードから挿入する攻撃メッセージ毎のランダムな送信時間間隔の選択範囲を示す．

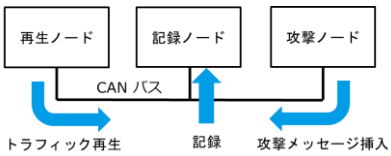


図 11．攻撃メッセージを含んだトラフィックの作成

表 3．攻撃メッセージの挿入条件

番号	周期攻撃間隔	不定期攻撃間隔
1	1s	0~1s
2	0.5s	0~0.5s
3	0.1s	0~0.1s
4	0.01s	0~0.01s

6.1.1 試験車両で取得したトラフィックデータ

表 4 に試験車両で取得した 8 種類のトラフィックデータを示す．これらのデータは一台の試験車両を用いて取得した．「ギアシフト」にはデータ取得の際に主に使用したギアシフトの位置を，「ドライブ」，「リバース」，「エンジンブレーキ」または「パーキング」の何れかで示す．「ドライブ」は前方，「リバース」は後方走行用のギアであり，「エンジンブレーキ」は速度に対して低いギア比の前方走行用のギアであり，「パーキング」はギアを固定するものである．試験車両のギアシフトには，これらの他にギアを開放する「ニュートラル」があるが，このギアシフトは 1～7 番のデータの記録開始時や終了時に含まれる．「目標速度」はデータ取得時に目標とした走行速度である．「灯火操作」にはヘッドライトの操作の有無を示す．「有り」の場合は，ヘッドライトをハイビームで一時的に点灯させるパッシング操作を繰り返し行った．

表 4．トラフィックデータ取得条件

番号	ギアシフト	目標速度	灯火操作
1	ドライブ	20	無し
2	ドライブ	40	無し
3	ドライブ	60	無し
4	エンジンブレーキ	60	無し
5	ドライブ	80	無し
7	リバース	20	無し
8	パーキング	0	有り

6.2 評価基準

本評価には次に示す 3 つの評価基準を用いた．車両データモデルの評価や，スレッショルドの決定等のパラメータ調整には数式(4)に示す False Positive Rate（FPR）を用いた．検知率の評価には，数式(5)に示す適合率と，数式(6)に示す再現率を用いた．適合率は検知結果に含まれる攻撃メッセージの割合を示し，1.0 に近い程攻撃メッセージと正常メッセージを正しく区別出来ることを意味する．再現率は全攻撃メッセージに対する検知した攻撃メッセージの割合を示す．1.0 に近い程，攻撃メッセージの認識率が高い．検知器において再現率，適合率共に 1.0 が理想的である．

$$FPR = \frac{偽陽性}{偽陽性 + 真陰性} \quad (4)$$

$$適合率 = \frac{真陽性}{真陽性 + 偽陽性} \quad (5)$$

$$再現率 = \frac{真陽性}{真陽性 + 偽陰性} \quad (6)$$

真陰性：正常メッセージが正常メッセージとして検出された数
偽陽性：正常メッセージが異常メッセージとして検出された数

真陽性：異常メッセージが異常メッセージとして検出された数
偽陰性：異常メッセージが正常メッセージとして検出された数

6.3 比較方式

比較対象には，イベント監視において一般的なメッセージの受信頻度を監視する方式を用いた．この方式では，単位時間に受信されるメッセージの数がスレッショルドを超えた場合に「異常」として検知する．受信メッセージの数を集計する単位時間を「累積時間」と定義する．またスレッショルドの決定は，学習用のトラフィックから得られる受信頻度の最大値を用いる．

6.4 パラメータ調整

ペイロード監視方式のパラメータ調整では，車両データモデルの学習を 6.4.1 節に示す様に行った．周期監視方式と比較方式のパラメータ調整では，スレッショルドの調整を 6.4.2 節に示す様に行った．

6.4.1 ペイロード監視方式の車両データモデルの学習

「シフトギア」の状態データに対する車両データモデルの学習を行った．この状態データは，ギアの状態をパーキング，ニュートラル，ドライブ，エンジンブレーキ，リバースの 5 つの値で示す．車両データモデルを最適化するため，学習に使用する相関制御データを表 5 に示す 5 種類で変更した．これら 5 種類の相関制御データは，トラフィックデータから相関制御データを抽出する際の相互相関係数の範囲が異なる．「抽出条件」には抽出する相互相関係数の範囲を示し，「抽出数」には各条件で抽出した相関制御データの数を示す．最適な車両データモデルは，表 4 に示す車両で取得した正常メッセージで構成されるトラフィックデータの FPR を測定し，これが最も小さくなるものを選択した．また参考のため，各モデルの大きさを決定木の深さで測定した．

測定結果を図 12 に示す．横軸の「車両データモデル番号」は表 5 に示す相関制御データの番号に対応する．学習用の相関制御データに相互相関係数 0.9 以上の制御データが含まれるモデル 1，2 の FPR が 10^{-5} と他の 3 つのモデルよりも一桁小さくなった．また決定木の深さも他の 3 モデルより浅く，モデルを小さくすることが出来た．モデル 1 と 2 を比較すると，モデル 1 の FPR が低く，モデルも小さい．モデル 1 では，学習時の相互相関係数が 0.9 よりも低い相関制御データを学習時に参照している．これは，学習に用いる一部の相関制御データの相互相関係数が低くとも，監視対象状態データの部分的な振る舞いに関連があれば，車両データモデルの FPR の抑制が可能であることを示す．学習用の相関制御データには，相互相関係数が 0.9 以上となる制御データを含ませると共に，相互相関係数が小さくとも多くの制御データを含ませるべきである．システム設計者の意見に基づき，監視対象状態データと関係性がある制御データを，学習用の相関制御データ群に追加すること等も，モデルの FPR 抑制に効果的である．

最適な車両データモデルにはモデル 1 を選択した．

表 5．相関制御データ抽出条件と抽出数

番号	抽出条件	抽出数
1	±1.0~±0.4	139
2	±0.9~±0.4	117
3	±0.8~±0.4	114
4	±0.6~±0.4	79
5	±1.0~±0.9	22

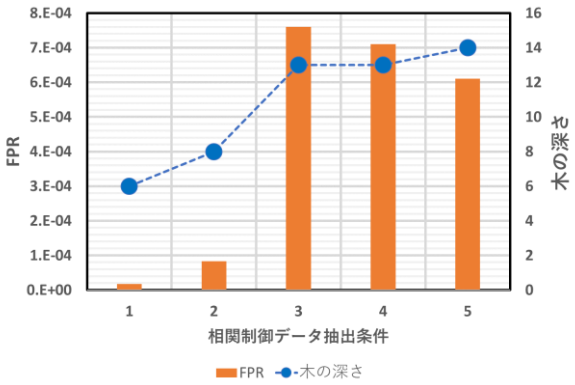


図 12．車両データモデルの FPR と決定木の深さ

6.4.2 スレッショルドの調整

周期監視方式と比較方式のスレッショルドは，「ヘッドライト」の状態データを含むイベントメッセージにより調整した．この状態データは，ヘッドライトの点灯状態を ON, OFF で示す．また，この状態データを含むイベントメッセージは，状態データの値が変化する毎に発生する．このメッセージに対するスレッショルドの調整には，表 4 に示す 8 番目のトラフィックデータを用いた．本データでは，試験者がヘッドライトの点灯，消灯を，可能な限り素早く繰り返し行った．

周期監視方式のスレッショルドの調整はウィンドウサイズを 10，20，30 の 3 種類で変更し，11 番データに対する FPR が 0 となる様に行った．比較方式のスレッショルド調整は累積時間を 0.01 とし，11 番データに対する FPR が 0 となる様に行った．表 6 に調整結果を示す．「提案手法」には周期監視方式において，ウィンドウサイズを 10，20，30 と変更した場合に各々で FPR が 0 となる最大自己相関係数をスレッショルドとして示した．「従来手法」には，式累積時間での受信頻度の最大値を，比較方式のスレッショルドとして示した．

表 6 スレッショルド

	従来手法	提案手法		
		10	20	30
スレッショルド	13	±0.95	±0.92	±0.90

6.5 評価結果

図 13 に提案手法と比較手法の再現率を示す．周期攻撃と不定期攻撃各々における攻撃メッセージの挿入時間間隔を横軸に取り，各攻撃メッセージの挿入時間における再現率を示す．周期監視方式の結果は「周期 10」，「周期 20」，「周期 30」に示す．各々の数字はウィンドウサイズを示す．

ペイロード監視方式の結果は「ペイロード監視(モデル１)」に示し，車両データモデルにモデル１を使用した．同様に図 14 には適合率の結果を示す．

ペイロード監視方式は周期攻撃，不定期攻撃において再現率，適合率で 1 に近い値を示しており，ほぼ全ての攻撃メッセージを正常メッセージと区別して検知できる．これに対し周期監視方式では，ウィンドウサイズに依存するが，周期攻撃については全ての攻撃メッセージ挿入時間に対し再現率が 1 に近い値を示した．比較方式については，周期攻撃の攻撃挿入間隔が 0.01s の時のみ再現率が 1 に近い値を示したが，それ以外は 0 となった．周期監視方式は周期攻撃に対し，比較方式では検知が困難な攻撃メッセージの挿入時間間隔が長い場合でも検知可能であるが，いずれの方式も再現率を示す場合の適合率は 0.5 で，攻撃メッセージと正常メッセージの区別ができない．また周期監視方式について，不定期攻撃で再現率は 0 であった．これは周期監視方式では，不定期攻撃の検知が困難なことを意味する．

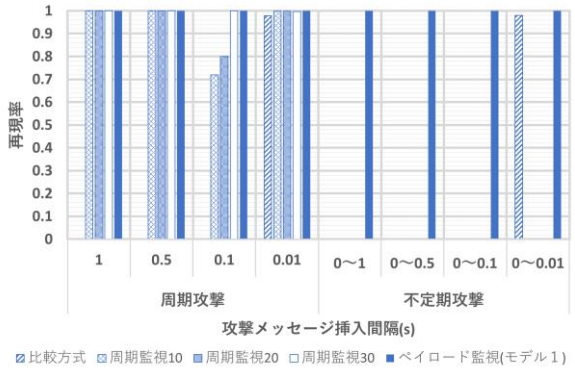


図 13．周期攻撃と不定期攻撃の再現率

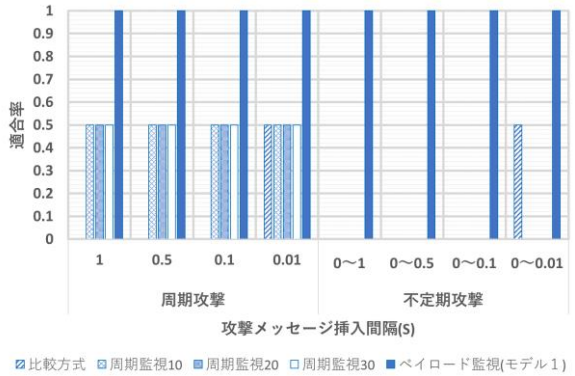


図 14．周期攻撃と不定期攻撃の適合率

7. まとめ

イベントメッセージに対する攻撃検知について 2 つの手法を提案し，攻撃検知率を確認した．一つはペイロード監視方式であり，イベントメッセージに含まれる状態データを監視する．本方式では頻度を監視する従来方式では困難な，攻撃を受けた際に正常メッセージと攻撃メッセージを区別することが可能である．また，周期攻撃，不定期攻撃いずれも検知可能である．もう一つは周期監視方式であり，イベントメッセージの現在と過去の自己相関係数を監視する．この方式では，頻度を監視する従来方式では困難な，攻撃挿入時間が長い周期攻撃の検知が可能である．

おわりに，２つの提案方式の利用方法を示す．サイバー攻撃に対して遅延応答を行う場合には，周期監視方式を用いて，誤検知は多くとも攻撃メッセージを見逃さずに検知する．検知結果から誤検知を選別する必要がある場合や，サイバー攻撃に対して即時応答が必要な場合には，ペイロード監視方式を併用するか，または周期監視方式に置き換えて用いる．

今後は，周期監視方式で検知が困難であった不定期攻撃について，検知方法の検討を行う．

参考文献

[1] Miller, C., and Valasek, C., “Remote Exploitation of an Unaltered Passenger Vehicle,” presented at DEF CON 23, August 2015.

[2] Müter, M., and Asaj, N., “Entropy-Based Anomaly Detection for In-Vehicle Networks,” *2011 IEEE Intelligent Vehicle Symposium (IV)*, 2011.

[3] Otsuka, S., Ishigooka, T., Oishi, Y., and Sasazawa, K., “CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems,” SAE Technical Paper 2014-01-0340, 2014.

[4] Hamada, Y., Inoue,M, Ueda, H., Miyashita, Y, et. al., “Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks,” SAE International Journal of Transportation Cybersecurity and Privacy, Vol1, 2018.

[5] International Organization for Standardization, “Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1, Rev. 2003.

[6] International Organization for Standardization, “Road vehicles-Controller area network (CAN) - Part 1: Data link layer and physical signaling,” ISO11898-1, Rev. 2015.

[7] Koscher, K., Czeskis, A., Roesner, F., Patel, S. et al., “Experimental Security Analysis of a Modern Automobile,” *2010 IEEE Symposium on* Security and Privacy , 2010.

[8] Larson, U.E., Nilsson, D.K., and Jonsson, E., “An Approach to Specification-Based Attack Detection for In-vehicle Networks,” *2008 IEEE Intelligent Vehicle Symposium,* 2008

[9] Markovitz, M. and Wool, A., “Field Classification, Modeling and Anomaly Detection in Unknown CAN Bus Networks,” presented at the 13th escar Europe Conference, November 11–12, 2015.

[10] Wasicek, A., Pesé, M., Weimerskirch, A., and Burakova, Y. et al., “Context-aware Intrusion Detection in Automotive Control System,” presented at the 5th escar USA Conference, USA, June 21–22, 2017.

[11] Hamada, Y., Inoue, M., Tateishi, H., Adachi, N., et. al., “Virtual Secsing Anomaly Detection for In-Vehicle Network,” 2018 Symposium on Cryptography and Information Security, January, 2018.

[12] Tsurumi, J., Kishikawa, T., Sasaki, T., Takahashi, R., et. al., “Proposal of Anomaly Detection Method for In-Vehicle Network based on Relation between Flag type Data,” 2017 Symposium on Cryptography and Information Security, January, 2017.

[13] Kuwahara,T., Baba, Y., Kashima, H., Ujiie, Y., “Statistical Anomaly Detection Based on CAN Message Frequencies”, 2016 Sumposium on Cruptography and Information Security, January, 2016.

[14] Breiman, L., J. Friedman, R. Olshen, and C. Stone. Classification and Regression Trees. Boca Raton, FL: CRC Press, 1984.