車載LANにおける異なる種類のデータフィールド値の関係に基づく異常検知方式

鈴木陵馬[1] 金森健人[2] 家平和輝[1] 井上博之[2] 石田賢治[2]

概要： 車載LANで広く利用されているCANはプロトコルの性質上，リプレイ攻撃に代表されるようななりすまし攻撃に脆弱である．なりすまし攻撃に用いられる異常メッセージに含まれるデータは，一緒に発生する他のメッセージに含まれる情報との間で整合性がとれなくなっている可能性が高い．すなわち，制御に用いられる情報が格納されているCANメッセージの中の，センサの具体的な数値等が格納されている領域であるデータフィールドの値がなりすまされた場合，関係するデータフィールドとの間で比較することで異常を検知できる可能性がある．本研究では，車載LANの複数の種類のデータフィールドの値の関係を算出することで，なりすまし攻撃を検知することを目的とする．提案方式では，メッセージのデータフィールドの役割毎にSensorフィールドとFlagフィールドに分類し，それらの値の関係より異常なメッセージを検知する．具体的には，Sensorフィールドの値が，Flagフィールドの値から算出される検知ルールの範囲内に収まっている場合を正規のメッセージとし，それ以外を異常メッセージとする．実車のトラフィックログを基にルールを作成し，車速を表すSensorフィールドの値がなりすまされた場合での異常検知率を求めた．FlagフィールドとSensorフィールドの関係を算出し，複数のFlagフィールドを使用することで，Sensorフィールドの値のなりすまし攻撃をより高い割合で異常を検知できることを確認した．

Anomaly Detection Method Based on Relation of Multiple Data Fields on In-vehicle Network

Ryoma Suzuki[1] Kento Kanamori[2] Kazuki Iehira[1] Hiroyuki Inoue[2] Kenji Ishida[2]

1. はじめに

車載LANで広く利用されているCAN（Controller Area Network）においては，広域網との常時接続サービスや無線接続機器の増加に伴い，車載LAN内のECUが外部から攻撃されるリスクが増加し，車載LANのセキュリティ保護の必要性が重要視されている．リプレイ攻撃に代表されるような単純ななりすまし攻撃に加えて，車載LANに対する新たな脅威としてバスオフ攻撃を用いたなりすまし攻撃が報告されている[1]．このような攻撃のなりすましメッセージに含まれる情報は，一緒に発生する他のメッセージの情報との間で整合性がとれなくなっている可能性がある．CANのメッセージには制御に用いられるデータが格納されており，センサの具体的な数値等が格納されている領域を本論文では，データフィールドと呼ぶ．データフィールド毎の値の変化を，関係するデータフィールドの間で比較することで異常を検知できる可能性がある．

本論文では，車載LANの複数の種類のデータフィールドの値の関係を算出することで，なりすまし攻撃による異常を検知する方式を提案する．提案方式では，メッセージのデータフィールドの役割毎にSensorフィールドとFlagフィールドに分類し，それらの値の関係より不正なメッセージを検知する．評価は実車トラフィックを用いて異常検知率を求めることで行う．評価の結果，複数のフラグフィールドを使用することで，より高い精度での異常検知が可能なことが明らかになった．

本論文の構成を以下に示す．2章では関連研究として従来の異常検知方式について述べる．次に3章では本論文にて提案する異常検知方式について述べる．4章では提案する異常検知方式の評価について述べる．5章ではまとめと今後の課題について述べる．

2. 関連研究

2.1 CANプロトコルの特徴とその攻撃手法

CANは車載LANで広く利用されている通信プロトコルである．CANの特徴としてバス型のネットワークを構成していることが一般的である．CANのメッセージフォーマットには識別子として使用されるCAN IDが含まれている．各ECUはバス上のメッセージのCAN IDによって，自身が受信すべきメッセージか確認するため，CAN IDは実質的な送信先アドレスとして扱われる．CANは送信元アドレスを持たず，共有バス上のブロードキャスト通信であるため，送信元のECUを識別することができず，盗聴およびなりすまし攻撃に対して脆弱である．

車載LANに対する様々な攻撃が報告されている．自動車の診断端子であるOBD-II端子を経由してCANにアクセスすることで，実際に車載LANに対しての攻撃の実現可能性を確認した研究[2]や，車載LANやECUに対する遠隔からのなりすまし攻撃の危険性を確認する攻撃検証用プラットフォームを開発し評価した研究[3]がある．なりすましメッセージにより先進運転支援システム（ADAS: Advanced Driving Assistant System）の自動ブレーキ機能をその作動条件を利用して無効化される可能性があることを確認している研究[4]がある．さらに，実車の車載測距センサを攻撃することで測距センサの機能停止やセンサ測定値を改ざんするなりすまし攻撃の実現可能性を示した例[5]もある．また，インフォテインメント機器の脆弱性を突いて，ファームウェアを書き換えることで遠隔からなりすましメッセージを送信

1 広島市立大学情報科学部
Faculty of Information Sciences, Hiroshima City University
2 広島市立大学大学院情報科学研究科
Graduate School of Information Sciences, Hiroshima City University

しエンジン，ステアリング，ブレーキ等の操作をされる可能性があることが発表され，約150万台の大規模リコールに繋がった事例[6]もある．

これらの事例では，CANバス上に正規のECU以外がなりすましメッセージを送信することで，車両の動作に影響を与えることを可能としている．このように正規のメッセージと攻撃メッセージが競合するなりすまし攻撃の方式をShared Busモデルと呼ぶ[7]．Shared Busモデルの攻撃では，正規の送信ECUも送受信を行っているため，あるCAN IDの単位時間あたりにおけるメッセージ数が増えることや，本来送信する正規のECU自身が送信していないにも関わらずそのCAN IDのメッセージを受信することから，比較的検知は容易である．一方，攻撃者が送信ECUの正規のメッセージの送信を停止した後で攻撃メッセージを送信することで，正規メッセージと攻撃メッセージが競合しないなりすまし攻撃の方式をOccupied Busモデルと呼び[7]，Shared Busモデルの攻撃と同様の方式での検知は困難である．

2.2 本研究で想定する攻撃

Occupied Busモデルのなりすまし攻撃としては，以下のようなものがある．送受信ECU間のサンプルポイントのずれを利用して，送信されたCANメッセージを送信ECUに検知されることなく，メッセージの内容を改ざんするなりすまし攻撃が報告されている[8]．また，バスオフ攻撃と呼ばれるCANの仕様のエラー制御を利用した攻撃も報告されている[9][10]．攻撃対象を意図的にバスオフ状態に遷移させた後になりすましメッセージを注入することで，正規の送信ECUに検知されないなりすまし攻撃が報告されている[1]．この方式では，送信ECU上に実装された異常検知方式[11]で検知が難しいことが示されている．これらのことから，Occupied Busモデルの攻撃におけるなりすまし攻撃の異常検知が必要となっている．

本研究では，車載LANの複数の種類のデータフィールドの値の関係を算出することで，ECUの乗っ取りや，正規メッセージの送信を停止させた後に攻撃メッセージを注入するようなOccupied Busモデルの攻撃におけるなりすまし攻撃を異常として検知することを目的とする．

2.3 従来の異常検知方式

CANに対するなりすまし攻撃の対策として，異常検知方式が研究されている．その内の一つとして，周期を基にした検知方式がある[12][13]．車両は制御システムであることから多くのメッセージがCAN ID毎に設定された周期で周期的に送信していることを基に検知を行っている．その周期に対して，一定のマージンを設定し，そのマージン外のメッセージやマージン内に2つ以上のメッセージが発生した場合に異常と検知している．この方式では正常メッセージが流れていない状態のなりすまし攻撃をされた場合，なりすましメッセージが正常状態と同じ周期で送信された場合検知できない．機械学習による検知方式も提案されている[14][15]．この方式では学習にデータ部の値の変化量を学習させることで，なりすましメッセージの注入によってデータ部が通常と異なる変化をした場合に検知が可能となる．しかし，この方式もなりすまし攻撃が行われた状態では正常メッセージが流れていることが前提となっており，正常メッセージの送信を停止させた後にリプレイ攻撃等正常状態と同じ変化でなりすましをされた場合には検知できない．

データフィールドをその特性ごとに分割し，それらをSensorやMulti-Value等の意味が異なるフィールドに分類し，異常検知に利用している研究がある[16]．Sensorは物理量の測定値を表すと考えられ，連続的でジッタやノイズのある値を表すフィールドを指す．Multi-Valueは少数の一意の値しか出現しないフィールドを表す．ここで提案されている異常検知方式では，センサ情報の種類毎に取りうる値の可変範囲を求め，その範囲に入るか入らないかを確認することで異常を検知する．しかし，この方式では可変範囲内で攻撃を行われる場合は検知が難しい．また，何かの状態を表すようなフラグ型データ（本論文におけるFlagフィールドと同等のもの）の異常を検知する方式も提案されており[17]，フラグ型データの遷移の異常を，遷移図を用いることで検知することを目的としている．相関データに着目した検知方式も提案されており[7]，相関のあるセンサデータを用いて攻撃検知対象の値を推測し，複数のセンサ情報を同時に監視することで異常を検知する方式である．高い精度で異常検知が可能であるが，相関のあるセンサ情報の組み合わせが，例えば車速であれば118個，エンジン回転数であれば78個と，多数のデータを使用する必要がある．

3. データフィールドの値の関係に基づく異常検知方式

3.1 概要

先行研究[7][17]を参考に，CANメッセージのペイロードにおいて，離散的な値を取り状態等を表すデータフィールドをFlagフィールドと呼び，連続的な値を取り値の大きさ等を表すデータフィールドをSensorフィールドと呼ぶ．先行研究[7]の異常検知ではSensorフィールドのみを用いており，Flagフィールドは特に考慮していない．SensorフィールドとFlagフィールドの関係性に着目し，複数を同時に監視することでセンサ値や制御情報のなりすまし攻撃をさらに高い精度で検出できる可能性がある．以下では，SensorフィールドとFlagフィールドの関係を基にしたSensorフィールドの値の異常検知方式について検討を行う．

本方式では，CANメッセージのペイロードに含まれるデータが，その役割ごとにSensorフィールドとFlagフィールドに分類されていることを前提に，それらの関係を監視することで異常検知を行う．まず，いくつかのSensorフィールドの値は，関係するFlagフィールドの値によりとりうる範囲が決まっていることが事前調査で分かった．図1に，車速を表すSensorフィールドの値と，あるフラグ値の関係の例を示す．FlagフィールドAの値であるフラグ値Aが01をとるとき，車速がとりうる範囲は0～10である．フラグ値Aが00をとるときは，車速はそれ以外の値をすべてとりうることを示している．また，フラグ値Bが010をとるとき，車速がとりうる範囲は0～10であり，フラグ値Bが001をとるとき，車速がとりうる範囲は20～40である．それ以外の車速に関しては，フラグ値

Bに関しては対応関係がないことを示している．

図2に提案する検知方式の処理の流れを示す．処理の流れとして大きく二つに分けることができる．まず，事前にルールの作成を行う．手順としては，Sensorフィールドの値がとりうる範囲を関係するFlagフィールドの値より算出し，その範囲を検知ルールとするというものである．次に，異常検知を行う．手順は，検知対象Sensorフィールドの値が検知ルールの範囲内に収まっている場合正規のメッセージとし，そうでない場合異常メッセージとするという流れである．以下の節にて詳細を記す．

3.2 異常検知アルゴリズム

3.2.1 事前準備

センサ情報およびフラグ情報とは，ある情報があるCAN IDのペイロード部分のどの位置に値が含まれているかという情報であり，それぞれSensorフィールドとFlagフィールドに対応する．なお，別途解析を行ったり仕様書を入手したりして，事前に対象とするセンサ情報やフラグ情報は分かっているものとする．事前準備として，ルール作成用車載トラフィックログ，センサ情報，フラグ情報を用意する．ルール作成用車載トラフィックログは，可能な限り多くのパターンのデータを使用して検知ルールが検知可能な範囲を大きくするために，様々な状態で運転した走行トラフィックのログであることが理想である．

3.2.2 Sensorフィールドに対するFlagフィールドの選択

あるSensorフィールドに対して，関係のあるFlagフィールドを選択する．1つのSensorフィールドに対して複数のFlagフィールドを選択することで，Flagフィールドによる状態の組み合わせが多くなる．その組み合わせ毎にSensorフィールドがとりうる範囲を限定できるので，複数のFlagフィールドを選択した場合，1つのFlagフィールドを選択した場合よりも，それぞれの状態によって限定されるSensorフィールドの値の範囲が狭くなる．つまり，検知ルール内の正規のメッセージであると判断する基準となる範囲を狭くすることができ，異常なメッセージのSensorフィールドの値が正規のものと近い値であっても検知できる可能性が上がる．その結果，異常検知の精度が高くなると考えられる．

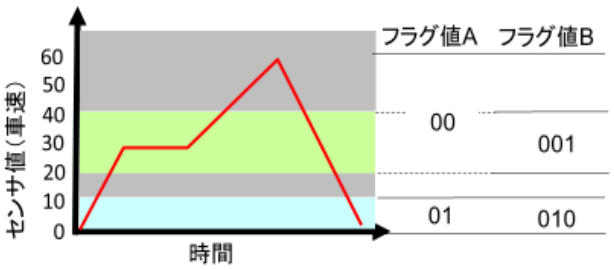

図1 センサ値と連携するフラグ値の関係

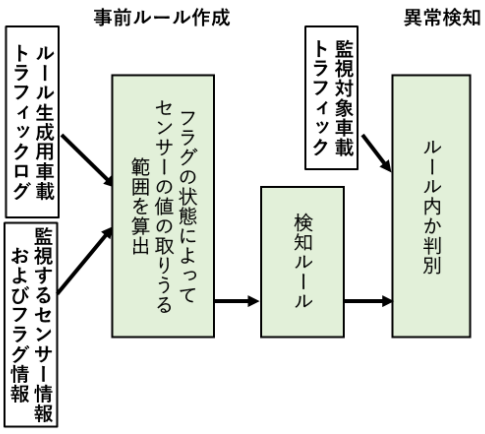

図2 提案する検知方式の流れ

3.2.3 ルール作成

ルール作成用車載トラフィックログを解析していくことでSensorフィールドの値のとりうる範囲を算出し，検知ルールとする．手順を以下に示す．

① ルール作成用車載トラフィックログに検知対象とするSensorフィールドのデータが現れた時に，同時にFlagフィールドがとっている値を対応付けて記録する．

② ルール作成用車載トラフィックログ内にてFlagフィールドがとる値の組み合わせすべてに対し，それぞれSensorフィールドがとりうる値の範囲を計算する．

上記で作成したSensorフィールドがとりうる値の範囲の組を検知ルールとする．

3.2.4 異常検知

異常検知の手順を以下に示す．

① 検知対象のトラフィックに検知対象とするSensorフィールドのデータが現れた時に，同時にFlagフィールドがとっている値を確認する．

② Flagフィールドがとっている値から，Sensorフィールドがとりうる値の範囲を，検知ルールから決定する．

③ 検知対象のSensorフィールドの値が，決定した範囲内であれば正常データと判断し，範囲外であれば異常データとして検知する．

このように検知対象データを検知ルールと比較することで異常検知を行う．

3.3 従来方式との違い

これまでOccupied Busモデルの攻撃におけるなりすまし攻撃に対応できる異常検知方式として，Sensorフィールドの相関関係を利用するものや，Sensorフィールドの値がとりうる範囲を計算しその範囲内に値が準じているかどうかで異常を検知するというものは存在した．本方式は，Sensorフィールドと関係のあるFlagフィールドの値をもとに，特定の状態でのSensorフィールドの値がとりうる範囲を限定することで，Sensorフィールドの値をより厳しく監視することができ，結果として高い割合で異常を検知できる可能性がある．

4. 評価と考察

4.1 評価に使用するデータと事前ルール作成

ルール作成用車載トラフィックログとして，実験用の車両をあるルートを往復30分間ずつ運転した車載LANトラフィックのログを2つ使用し，2通りの検知ルールを作成した．復路のログを元にしたものをルールA，往路のものをルールBとする．ルールAとBは走行経路は同じであるが，走行時の勾配や走行

時間帯が異なっており，ルールとしては同一ではない．

評価に使用したSensorフィールドに対し組み合わせたFlagフィールドを表1にまとめた．Sensorフィールドとして車速を使用し，Flagフィールドとしてギアポジションとハイブリッドシステム情報を使用した．ルールAとルールBのそれぞれを用いて異常検知を行った．表2に，Flagフィールドの値があらわしうる状態についてまとめた．なお，Flagフィールドの状態は解析の結果推定したものである．評価において作成した検知ルール，すなわちFlagフィールドの値によって限定されるSensorフィールドの値の範囲の関係を表3にまとめた．なお，ここでは評価において確認したもののみをまとめてある．また，ルール作成用車載トラフィックログで現れなかったフラグの組み合わせに対しては，“-”で表現している．

検知方式の評価として，車速を表すCANメッセージのSensorフィールドがなりすまされた場合を想定した評価用データを用意した．評価用データは，ルールBを作成する際に使用した車載トラフィックログから，Sensorフィールドがすべて0以外の値をとる連続した区間を1分40秒間取り出し，検知対象Sensorフィールドの値をなりすましの内容に応じて変更することで作成した．具体的には，車載トラフィックログ内の車速を表すデータフィールドの値をすべて元の値の定数倍になりすまされたという状況を再現した．ここで，評価用データに検知対象Sensorフィールドが現れた時に，その値がFlagフィールドの値をもとに限定した範囲内であるかどうか確認することで異常検知を行った．なお，実験用の車両としては，以前にCANメッセージを解析済みである国産ハイブリッド自動車[3]を使用した．

4.2 異常検知の評価

本論文では，異常検知を評価する際の基準として，再現率を異常検知率としている．再現率とは，網羅性を判定する指標であり，ここでは異常なデータ全体に対し，正確に異常と判断できた数の割合のことを指す．提案する方式は，Bus上に正規メッセージが流れず，異常メッセージのみが流れるOccupied Busモデルの攻撃で発生する異常に対する検知を目的としており，この場合の異常検知の評価には再現率を用いることが最も適切であると考える．また，評価用データはSensorフィールドが0以外の値をとる車載トラフィックログのデータフィールドの値をすべて定数倍して作成しているので，評価用データ内の検知対象Sensorフィールドの値はすべて攻撃データであるといえる．

図3に車速における評価用データの倍率ごとの異常検知率の変化を，ルールAとルールBのそれぞれについてまとめたグラフを示す．また，Flagフィールドとしてギアポジションの1つのみを使用し，ルールAを用いて異常検知を行った．その結果と，図3のルールAを用いたものを比較したグラフを図4に示す．

4.3 結果と考察

評価の結果，倍率が1倍の時，すなわち攻撃されていないとする評価用データにおいて，ルールAにおいては0.69パーセントの割合で正常なデータを異常と判断していた（図3）．この誤検知について解析したところ，検知ルール内のSensorフィールドの値の範囲の上限を上回る値が評価用データに存在することが分かった．車載トラフィックログから検知ルールを作成する本方式では，ルール作成用車載トラフィックログとして，どのような運転をしたものを使用するかが重要となる． そのため3.2.1節で述べたように様々な状態で運転した走行トラフィックログを用いることが重要である．また，評価用データを作成する際の倍率が1より大きい時と小さい時で異常検知率が大きく異なっていることがわかる．これは，前者では検知ルール内のSensorフィールドの値の範囲の上限を超えるものが異常と判断されているのに対し，後者では，異常データが正規のSensorフィールドの値の範囲内に入ってしまっており，3.2.2節で述べた，正規のメッセージであると判断する基準となる範囲が広

表1 Sensorフィールドに対し組み合わせたFlagフィールド

Sensorフィールド	Flagフィールド
車速	ギアポジション ハイブリッドシステム状態

表2 本研究で用いたFlagフィールド

Flagフィールド	取りうる値
ギアポジション情報	0000: パーキング(P) 0001: リバース(R) 0010: ニュートラル(N) 0011: ドライブ(D)
ハイブリッドシステム情報	0100: 停車 0110: 駐車後退 1000: エンジンとバッテリーを動力に走行中 1001: エンジンのみを動力で走行中 1100: バッテリーのみを動力で走行中 1110: 不明 1111: バッテリー充電中

表3 評価におけるルール

ギアポジション情報	ハイブリッドシステム情報	車速の値の範囲 ルールA	車速の値の範囲 ルールB
0000	0110	0～0	0～0
0000	1110	0～0	-
0001	0100	0～0	-
0001	0110	0～342	0～377
0010	0100	0～0	-
0010	0110	-	0～176
0010	1110	0～0	-
0010	1111	-	184～271
0011	0100	0～523	0～521
0011	0110	0～0	-
0011	1000	1321～6329	1370～7563
0011	1001	1987～5101	1918～5491
0011	1100	197～6803	271～7518
0011	1111	170～6315	188～7426

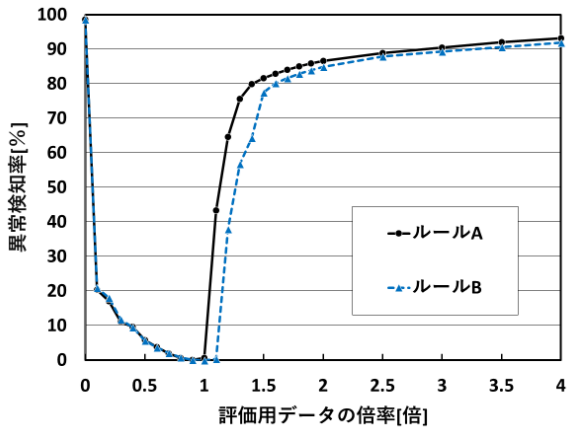

図3 車速における異常検知率の変化

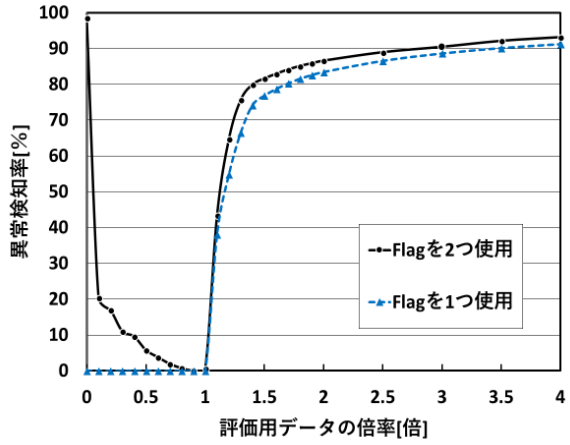

図4 使用するフラグ数による異常検知率の違い

すぎることを示している.

図4に示すように，フラグを1つのみ使用して検知を行った場合より，複数使用した場合のほうが異常検知率は高い．特に，評価用データの倍率が0倍から1倍の領域にかけて顕著に違いが現れていることがわかる．これは，使用するフラグの数を増やすことで，正規のメッセージであると判断する基準となる範囲を狭くできることの根拠となる.

評価において利用可能であったデータフィールドは，CANトラフィックを解析することで得られたもののみであった．そのため，Flagフィールドとして利用したデータフィールドが2つのみであり，高い割合で異常を検知はできなかった．しかし，Flagフィールドの選択をより理想的に実行できればさらに高い精度で検知可能である可能性を示した.

また，評価を通じて，さらに検知精度を向上させるための方針が得られた.

- 利用可能なFlagフィールドを増やし，より多くのFlagによる状態を考慮することで，正規のメッセージであると判断する基準となる範囲を狭くする.
- Sensorフィールドに対するFlagフィールドの選択をアルゴリズムで表現し，最も効率の良い組み合わせをどの車種のデータを用いても選択可能にする.
- 今回提案した方式ではSensorフィールドの値を大きさという観点のみから判断している．前後のSensorフィールド値の状態から変化量を計算し対応付けることで使用できるFlagフィールドの種類の幅を広げる.

5. おわりに

車載LANのCANメッセージのデータフィールドにおけるFlagフィールドとSensorフィールドの関係を算出し，複数のFlagフィールドを使用することで，Sensorフィールドの値のなりすまし攻撃をより高い割合で検知できる異常検知方式を提案した．今後の課題として，より多くのFlagフィールドを使用することによる異常検知率の変化を求めるなどして，最適なFlagフィールドの組み合わせを調査することが挙げられる.

謝辞

本研究の一部は，JSPS科研費18K11299，および広島市立大学特定研究費により行われた．ここに記して謝意を表す.

参考文献

[1] K. Iehira, H. Inoue, and K. Ishida, “Spoofing Attack Using Bus-off Attacks against a Specific ECU of the CAN Bus,” IEEE Consumer Communications & Networking Conference2018（CCNC2018）, pp.208-211, Jan. 2018.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,” Proc. 2010 IEEE Symposium on Security and Privacy, pp.447-462, May 2010.

[3] T. Ezaki, T. Date, and H. Inoue, “An Analysis Platform for the Information Security of In-vehicle Networks Connected with the External Networks,” The 10th International Workshop on Security (IWSEC2015), Advances in Information and Computer Security (LNCS 9241), pp.301-315, Aug. 2015.

[4] 中野将志，中澤祐希，久保田貴也，汐崎充，藤野毅，“ADAS ECUの動作条件を悪用した自動車の衝突回避システムに対する攻撃手法と軽量MAC認証手法の提案，”暗号と情報セキュリティシンポジウム2016 (SCIS2016), 8pages, Jan. 2016.

[5] 中澤祐希，中野将志，汐崎充，久保田貴也，白畑正芳，藤野毅，菅原健，鈴木大輔，小林信博，“車載測距センサに対するセキュリティ評価，”暗号と情報セキュリティシンポジウム2016 (SCIS2016), 8pages, Jan. 2016.

[6] C. Miller, and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA 2015, pp.1-91, Aug. 2015.

[7] 濱田芳博，井上雅之，立石博志，足立直樹，上田浩史，宮下之宏，礒山芳一，畑洋一，“相関データによる車両データモデルを用いた車載ネットワーク向けアノマリ検知，”暗号と情報セキュリティシンポジウム2018(SCIS2018), 8pages, Jan. 2018.

[8] 松本勉，中山淑文，向達泰希，土屋遊，吉岡克成，

“CANにおける再同期を利用した電気的データ改ざん，”暗号と情報セキュリティシンポジウム2015 (SCIS2015), 8pages, Jan. 2015.

[9] K. T. Cho, and K. G. Shin, “Error Handling of In-vehicle Networks Makes Them Vulnerable,” Proc. 2016 ACM SIGSAC CCS2016, pp.1044-1055, Oct. 2016.

[10] 亀岡良太，久保田貴也，汐崎充，白畑正芳，倉地亮，藤野毅，“ラズベリーパイからのスタッフエラー注入によるCAN ECUへのバスオフ攻撃，”暗号と情報セキュリティシンポジウム2017(SCIS2017), 8pages, Jan. 2017

[11] 畑正人，田邉正人，吉岡克成，松本勉，“CANにおける不正送信阻止方式の実装と評価，” 電子情報通信学会技術研究報告, vol.112, no.342, pp.15-22, Dec. 2012.

[12] 矢嶋純，長谷部高行，“CANの周期送信メッセージに対する攻撃検知手法の詳細評価とその評価手法，” 暗号と情報セキュリティシンポジウム2017(SCIS2017), 8pages, Jan. 2017.

[13] 倉地亮，高田広章，上田浩史，堀端啓史，“車載制御ネットワークにおける送信周期監視システムの提案，”暗号と情報セキュリティシンポジウム2015(SCIS2015), 7pages, Jan. 2015.

[14] 高橋良太，佐々木崇光，松島秀樹，芳賀智之，岸川剛，鶴見淳一，“Sand Sprinkled Isolation Forestによる車載セキュリティ向け異常検知の精度向上”暗号と情報セキュリティシンポジウム2017(SCIS2017), 6pages, Jan. 2017.

[15] 手柴瑞基，井上博之，石田賢治，“車載セキュリティゲートウェイにおける機械学習を用いた動的フィルタリング機構の実装と評価,” 信学技報 IN2016, vol.116, no.485, pp.205-210 Mar. 2017.

[16] M. Markoviz，and A. Wool，“Field Classification，Modeling and Anomaly Detection in Unknown CAN Bus Networks,” escar Europe Conference, Nov. 2015.

[17] 鶴見淳一，岸川剛，佐々木崇光，高橋良太，芳賀智之，松島秀樹，“フラグ型データの関係に基づいた車載ネットワーク向け異常検知手法の提案，”暗号と情報セキュリティシンポジウム2017(SCIS2017), 6pages, Jan. 2017.