情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.8　No.2　1–12 (May 2018)

推薦コンシューマ・デバイス論文

特定のCANメッセージを送信するECUに対するバスオフ攻撃を利用したなりすまし攻撃

家平 和輝[1,a)]　井上 博之[2,3]　石田 賢治[2]

受付日 2017年9月30日, 採録日 2018年2月20日

概要：車載 LAN で広く使われている CAN は共有バス型のネットワークトポロジで暗号化や認証の仕組みも標準化されておらず，なりすましメッセージの注入や ECU を無効化するバスオフ攻撃を実施することで ECU や車載器が不正な動作を行うことが報告されている．正規の送信 ECU でなりすまし攻撃を検知する方式や，メッセージの受信周期に着目した攻撃検知方式等が提案されており，既存のなりすまし攻撃を検知可能であることも報告されている．従来の攻撃検知方式では検知できない攻撃が考案されると，新たな脅威となる．本研究では，バスオフ攻撃を用いて正規の送信 ECU の送受信を完全に阻止し，かつ周期が同じなりすましたメッセージを注入することで，既存の検知方式では検知できないようななりすまし攻撃を提案する．CAN バスの信号を直接操作するために FPGA を用いて攻撃装置を実装し，実験室での模擬環境および実車で本攻撃の評価実験を行い，提案方式の有効性を確認した．

キーワード：車載 LAN，CAN，なりすまし攻撃，バスオフ攻撃

A Spoofing Attack Using Bus-off Attacks to a Specific ECU on the CAN Bus

Kazuki Iehira[1,a)]　Hiroyuki Inoue[2,3]　Kenji Ishida[2]

Received: September 30, 2017, Accepted: February 20, 2018

Abstract: The Controller Area Network (CAN), which is widely used in in-vehicle network, constitutes a shared-bus network topology and has no standardized encryption and authentication mechanisms. Therefore, Electronic Control Units (ECUs) and in-vehicle devices can perform illegal actions by spoofing message injections or bus-off attacks. Countermeasures have been proposed, such as detecting spoofing attacks with a legitimate transmitting ECU and an attack detection method that focuses on a message is sending cycle. Existing spoofing attacks can be detected. In this study, we propose a spoofing attack that cannot be detected by existing detection method. We completely block transmission and reception of legitimate transmitting ECUs using the bus-off attack and by injecting spoofed messages with the same cycle. We implemented an attack device using a field programmable gate array (FPGA) to directly manipulate the CAN bus signal, and conducted this attack in a laboratory environment and in an actual vehicle, and confirmed the effectiveness of the proposed method.

Keywords: in-vehicle LAN, CAN, spoofing attack, bus-off attack

1. はじめに

車載 LAN で広く使われている CAN（Controller Area Network）[1] は共有バス型のネットワークトポロジをと

[1] 広島市立大学情報科学部
Faculty of Information Sciences, Hiroshima City University, Hiroshima 731–3194, Japan
[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, Hiroshima 731–3194, Japan
[3] 重要生活機器連携セキュリティ協議会研究開発センター
Connected Consumer Device Security Council (CCDS), Naha, Okinawa 900–0005, Japan
[a)] iehira@net.info.hiroshima-cu.ac.jp

本論文の内容は 2017 年 6 月のマルチメディア，分散，協調とモバイルシンポジウムにて報告され，コンシューマ・デバイス&システム研究会主査により，情報処理学会論文誌コンシューマ・デバイス&システムへの掲載が推薦された論文である．

り，メッセージの暗号や送信元の認証の仕組みも標準化されていないため，盗聴やなりすまし攻撃に対して脆弱である．CAN における攻撃事例として，CAN バスになりすましメッセージを注入するなりすまし攻撃を実施することで ECU（Electronic Control Unit）や車載器が不正な動作を行うことを示した報告 [2], [3], [4] がいくつかある．そのため，なりすまし攻撃を検知し阻止する仕組みが必要とされている．なりすまし攻撃の対策として，MAC（Message Authentication Code）を付加して送信元 ECU を認証する方式 [5] やメッセージを暗号化する方式 [6] が提案されている．しかし，CAN では 8 byte しかデータ部を持たず，伝送速度も最大 1 Mbps と低速であるため，CAN の仕様を変更することなく実現するのは難しい [7] とされている．CAN の仕様を変更することなく実現可能ななりすまし攻撃検知方式として，CAN の周期性に着目した受信 ECU での攻撃検知方式 [8] や正規の送信 ECU で自身が送信したものでないなりすましメッセージを検知する方式 [9] が提案され，なりすまし攻撃を検知可能であることが報告されている．これまでに提案されている攻撃検知方式により検知できない攻撃が考案されると，車両や乗員にとって新たな脅威となる．本研究では，正規の送信 ECU および受信 ECU で検知できない攻撃を提案する．正規の送信 ECU での攻撃検知と正規メッセージが CAN バスに流れることを阻止するために，正規の送信 ECU の送受信を阻止する．同時に，周期をなりすましたメッセージを注入することで，受信 ECU でも検知できないなりすまし攻撃を提案する．提案方式を模擬環境と実車で評価し，新たな脅威になりうるかの考察を行う．

以降では，まず 2 章で関連研究について述べ，3 章で提案する攻撃方式の原理について述べ，4 章でその実装と評価について述べ，5 章で考察を行う．最後に 6 章でまとめを行う．

2. 関連研究

2.1 CAN プロトコルの特徴

CAN では，CAN バスを構成する 2 本の信号線を用いた差動通信を行っている．CAN コントローラで送受信処理およびエラー制御等を行い，CAN トランシーバで差動通信を行う．信号線に電圧差がなく論理 “1” を表す状態をリセッシブ，電圧差があり論理 “0” を表す状態をドミナントと呼ぶ．もしリセッシブとドミナントが同タイミングで送信されると，ドミナントが優先される．CAN では同じ論理のビットが連続して送信されることで同期がとれなくなることを防ぐためにビットスタッフィングルールを適用している．そのため，同じ論理のビットが 5 bit 連続するときは論理を反転したビットを 1 bit 挿入することが定められている．CAN メッセージは送信元アドレスを持たず，宛先アドレスを表す CAN ID しか持っていない．さらに，

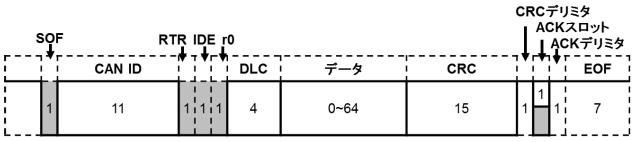


図 1　データフレームのフォーマット
Fig. 1　The format of a data frame.

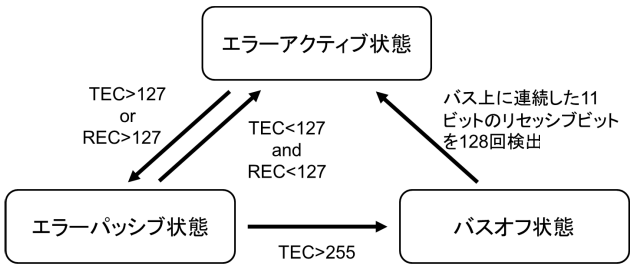


図 2　ECU の状態と遷移条件
Fig. 2　ECU state and the transition condition.

CAN メッセージは共有バス上でブロードキャスト通信されるため，送信元を知る手段がない．

通常のデータを送信するメッセージをデータフレームと呼び，データフレームは**図 1** に示すように主に CAN ID と DLC（Data Length Code）とデータ部から構成される．エラーを周知させるメッセージをエラーフレームと呼び，6 bit のエラーフラグと 8 bit のエラーデリミタ（リセッシブ）から構成される．特に，エラーフラグが 6 bit のドミナントから構成されるものをアクティブエラーフレームと呼び，エラーフラグが 6 bit のリセッシブから構成されるものをパッシブエラーフレームと呼ぶ．

エラー制御方法として，ECU がエラーを検出するとエラーフレームを送信することで，エラーの発生を周知させる．エラーの種類として，送信したビット論理と受信したビット論理が異なるときに発生するビットエラーやビットスタッフィングルールを無視したことを検出したときに発生するスタッフエラーや固定フォーマットのビットフィールドの改ざんにより発生するフォームエラーなどがある．アクティブエラーフレームが送信されたとき，ビットスタッフィングルールへの違反，または固定フォーマットのビットフィールドを改ざんし，他の ECU ではスタッフエラーまたはフォームエラーを検出する．パッシブエラーフレームが送信されたとき，ビットスタッフィングルールを違反し，他の ECU ではスタッフエラーを検出する．CAN コントローラではエラーを検出すると，送信エラーカウント（TEC）または受信エラーカウント（REC）の値を増加させる．特に，送信者がビットエラーまたはスタッフエラーを検出した場合は TEC が 8 増加する．CAN では，**図 2** に示す 3 つの状態が定められている．CAN コントローラはこれらの状態を持ち，TEC および REC の値に応じて状態が遷移する．**表 1** に示すように，状態に応じて

表 1　ECU におけるエラー状態に応じた送受信制限
Table 1　Restriction of sending and receiving according to the ECU error state.

状態	CAN バスへのアクセス制限	エラーフラグ
エラーアクティブ	なし	6bit のドミナント
エラーパッシブ	連続送信時に 8bit 期間の送信待機	6bit のリセッシブ
バスオフ	送受信の禁止	送信不可

バスへのアクセスが制限され，エラーフラグの値も変化する．エラーアクティブ状態は通常状態と定められており，制限はかからない．エラーパッシブ状態はエラーを起こしやすい状態と定められており，他の ECU の通信を妨げないために連続送信時の送信待機時間が通常より長く設定されている．さらに，エラー検出時もリセッシブのみを送信するため，他の ECU による送信を妨げることはできない．バスオフ状態はバス上の通信に参加できない状態と定められており，送受信のすべてを禁止されている．

2.2　ECU を無効化するバスオフ攻撃

2016 年に CAN における新たな脅威として，ビットエラーを誘発させることで，ECU をバスオフ状態に遷移させ CAN バスから離脱させるバスオフ攻撃 [10] が提案されている．また，エラーフレームを注入することにより，送信開始タイミングや周期といった時間的な制約のないバスオフ攻撃が 2 種類提案されている [11]．すなわち，現在提案されているバスオフ攻撃は 3 種類となる．ここでは，文献 [10] で提案されている方式をビットエラー誘発によるバスオフ攻撃と呼び，文献 [11] で提案されている 2 種類の方式は文献に従い，それぞれスタッフエラー注入によるバスオフ攻撃と 1 フレームでのバスオフ攻撃と呼ぶ．

ビットエラー誘発によるバスオフ攻撃では，ターゲットとする ECU にビットエラーを引き起こさせることで TEC を増加させる．攻撃手順として，以下の条件を満たすメッセージを正規メッセージと同時に送信する．

条件 1．ターゲット ECU と同一の CAN ID であること．
条件 2．ターゲット ECU の送信したリセッシブのビットに対して，攻撃者がドミナントのビットを送信する．ただし，これ以前のビットはすべて同一のものとする．

図 3 に示すように，ターゲット ECU と攻撃者が同時に送信を開始する．その後，送信ビットが異なるタイミングでターゲット ECU がビットエラーを検出し，TEC が 8 増加される．この攻撃を繰り返し行うことにより TEC を 255 より大きくして，ターゲット ECU をバスオフ状態に遷移させる．この攻撃では，攻撃者とターゲット ECU がエラーアクティブ状態であるときは，再送も同時に行われるため特に効果的に TEC を増加させられる．ターゲット ECU がエラーパッシブ状態であるときは，ターゲット ECU が送信したパッシブエラーフレームで攻撃者の送信を阻止することができないため，攻撃に用いたメッセージが CAN バスに送信される．この攻撃では，攻撃時に攻撃者の TEC も増加するため，攻撃者が特殊な CAN コントローラを利用しない限りは連続して攻撃を成功させることは難しい．

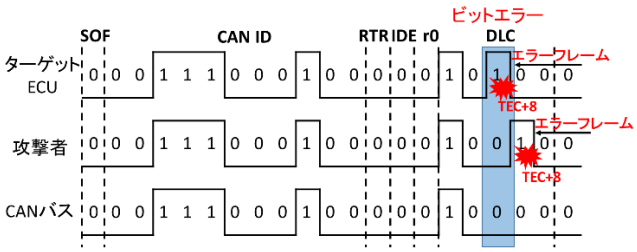


図 3　ビットエラー誘発によるバスオフ攻撃
Fig. 3　The bus-off attack using a bit error generation.

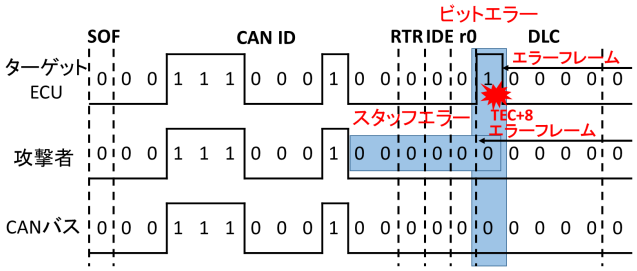


図 4　スタッフエラー注入によるバスオフ攻撃
Fig. 4　The bus-off attack using a staff error injection.

スタッフエラー注入によるバスオフ攻撃では，**図 4** に示すようにターゲット ECU が送信したメッセージをエラーフレームで無効化し，ターゲット ECU の TEC を増加させる．攻撃手順を以下に示す．

(1) データフレームの SOF の検出
(2) データフレームの CAN ID の読み取りと識別
(3) エラーフレームの送信

ターゲット ECU は攻撃者から送信されたエラーフレームによりビットエラーまたはスタッフエラーを検出し，TEC が 8 増加される．この攻撃を繰り返し行うことにより TEC を 255 より大きくして，ターゲット ECU をバスオフ状態に遷移させる．

1 フレームでのバスオフ攻撃では，スタッフエラー注入によるバスオフ攻撃で送信したエラーフレームの代わりに 260 bit のドミナントを送信する．**図 5** に示すように CAN の仕様よりエラー検出後にドミナントが 14 bit 期間続いていると TEC が 8 増加され，さらに続けてドミナントが 8 bit 期間続くごとに TEC が 8 増加される．これより，最短 255 bit（エラービット 1 bit + 14 bit + 8 bit × 30）期間続いたとき，TEC が 255 より大きくなりターゲット ECU はバスオフ状態に遷移する．ビットスタッフィングルールが適用されるため，6 bit 以上連続してリセッシブが送信さ

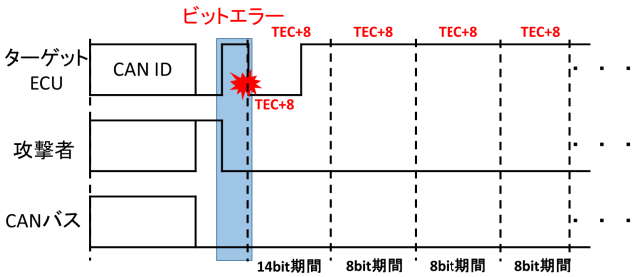


図 5　1 フレームでのバスオフ攻撃
Fig. 5　The bus-off attack in a single frame.

れることはない．6 bit（エラービット 1 bit + 5 bit）連続してドミナントを送信すると，確実にビットエラーを引き起こせる．以上より，260 bit 期間以上連続してドミナントを送信し続けることで確実にターゲット ECU をバスオフ状態に遷移させることができる．

ビットエラー誘発によるバスオフ攻撃では，正規メッセージと同じ CAN ID を持つ攻撃メッセージを送信する．ターゲット ECU がエラーパッシブ状態であるとき，攻撃メッセージを受信し攻撃を検知される可能性がある．スタッフエラー注入によるバスオフ攻撃と 1 フレームでのバスオフ攻撃は CAN バスへ物理的にアクセスする必要があるため，攻撃が可能となる条件は比較的厳しくなる．スタッフエラー注入によるバスオフ攻撃ではエラーフレームのみ送信する．エラーフレームの発生原因および送信元を特定することは原理的にできないため，攻撃を検知できない．1 フレームでのバスオフ攻撃では通常のエラーフレームより長い期間ドミナントを送信するため，スタッフエラー注入によるバスオフ攻撃よりは異常検知しやすいと考えられる．しかし，通常の ECU では CAN バスをメッセージ単位でしか監視できないため，これを検知するのは難しい．

2.3　既存のなりすまし攻撃

CAN における攻撃事例として，なりすましたメッセージを注入するなりすまし攻撃を実施することで，ECU や車載器が不正な動作を行う可能性があることが示されている [2], [3], [4] ことから，なりすまし攻撃は CAN における重大な脅威とされている．

なりすまし攻撃の中でも比較的単純な方式として，周期をなりすましたメッセージを注入する方式がある．この方式では，単純に CAN ID と周期をなりすましたメッセージを CAN バスに注入する．この方式では，正規メッセージも送信されているため，受信 ECU では通常時の 2 倍のメッセージを受信することになり，攻撃を検知されやすい．

通常，リセッシブとドミナントが同時に送信されたとき，ドミナントが優先される．これを覆す方法として，CAN バスを構成する 2 本の信号線を交差させることで，リセッシブとドミナントが同時に送信されたときにリセッシブが優先されるテクニックが報告されている [12]．このテクニックを利用して生成したデータフレームを用いることで，エラーフレームで送信を阻止することができないなりすまし攻撃が報告されている [13]．しかし，この方式も周期をなりすましたメッセージを注入する方式と同様に，正規メッセージも送信されるため，攻撃を検知されやすい．

送信 ECU と受信 ECU の CAN バスの論理値をサンプリングするタイミングすなわちサンプルポイントが異なるとき，タイミングよく CAN バスの値を改ざんすることで，正規の送信 ECU でビットエラーを検出されず，正規メッセージを改ざんするなりすまし攻撃 [12] が報告されている．この攻撃では，正規メッセージと同じ周期であり，正規の送信 ECU では改ざんされる前の値を受信するため，検知されることはない．しかし，この攻撃ではビットスタッフィングによりビット数が異なるメッセージになりすますことはできない．さらに，複数の ECU が 1 つの CAN バス上に接続された場合は，それぞれの受信 ECU のサンプリングポイントが異なるため，タイミング制約が厳しく実車両上での攻撃難易度が高く実現可能性が低いと考えられる．

エラーフレームで送信を阻止することができないなりすまし攻撃を行う方式は，なりすましメッセージの送信を阻止されないということを除けば，周期をなりすましたメッセージを注入する方式と同じである．すなわち，攻撃検知を議論する場合は，この 2 方式を同等に扱っても問題ない．サンプルポイントが異なるときにタイミングよく CAN バスの値を改ざんする方式は実現可能性が低いと考えられるため，本研究では議論の対象にしない．以上より，周期をなりすましたメッセージを注入する方式を既存のなりすまし攻撃として，以降の議論を行う．

2.4　CAN におけるなりすまし攻撃検知方式

ECU で得られる情報は，宛先を表す CAN ID とデータと受信周期のみである．受信したデータのみから次に受信するデータを予測することは現実的でなく，受信 ECU で送信元の ECU を知ることはできない．以上より，特別な改造をされた CAN コントローラを用いない ECU で攻撃を検知する方法は，正規の送信 ECU でなりすましメッセージを検知する方法，および受信 ECU で周期から検知する方法のみである．本研究において，特別な改造をされた CAN コントローラとは，1 フレームでのバスオフ攻撃で用いている連続 260 bit のドミナントのように CAN の規格で定義されていないフレームでの送受信が可能である．または，エラー状態の遷移条件を満たさない CAN コントローラとする．

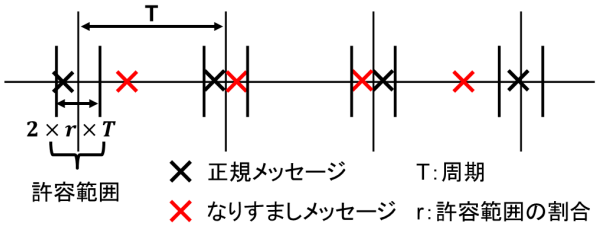
特定の CAN ID を持つメッセージを送信する ECU は同一の CAN バスに 1 台しか接続されないことを前提として，各 ECU で自身に割り当てられた CAN ID を持つなりすましメッセージが他から送信されると，正規の送信 ECU で

攻撃を検知する方式が提案されている [9]．しかしこの方式では，攻撃者により正規の送信 ECU でのメッセージ受信を阻止されると，検知できない．

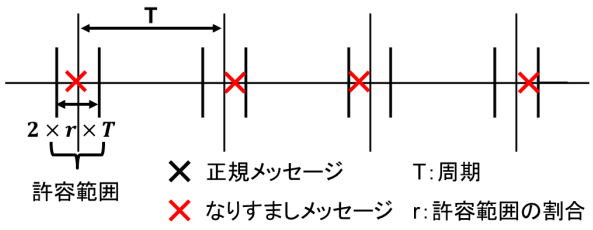
攻撃対象となる自動車は制御システムであることから，それぞれの ECU は CAN ID ごとに決められた周期でメッセージを送信することが多い．この性質に着目したなりすまし攻撃を検知する方式はいくつか提案されている [8], [14]．2 つの文献では，攻撃検知方式として同様のアルゴリズムをとっている．**図 6** (a) に示すように，周期性に着目した攻撃検知方式では想定される受信周期の前後に許容範囲を設ける．そこで，許容範囲内に 1 つだけメッセージを受信すれば攻撃はなかったものと判断する．許容範囲外で 1 つ以上のメッセージを受信するか許容範囲内で複数のメッセージを受信すれば攻撃があったものと判断する．この攻撃検知方式は，正規メッセージに加えてなりすましメッセージが送信されるという仮定に基づいている．そのため，図 6 (b) に示すように正規メッセージの送信を阻止して，なりすましメッセージを注入することができれば，周期性に着目した攻撃検知方式では検知できない攻撃が実現する．

エラーフレームを監視し攻撃検知を行う方式 [15] が提案されている．この方式により，エラーを頻発するビットエラー誘発によるバスオフ攻撃とスタッフエラー注入によるバスオフ攻撃は検知される可能性が高い．しかし，1 フレームでのバスオフ攻撃では正規のエラーフレームを用いずに CAN の規格で定義されていない 260 bit のドミナントをエラーフレームとして用いているため，この方式では検知することができないと考えられる．

本研究では，バスオフ攻撃と周期をなりすましたメッセージを注入する方式のなりすまし攻撃を組み合わせることで，なりすましメッセージに制限を持たず，タイミング制約も厳しくなく，正規の送信 ECU および受信 ECU で検知できないようななりすまし攻撃を提案する．



(a) 周期性に着目した攻撃検知方式で検知できる攻撃



(b) 周期性に着目した攻撃検知方式で検知できない攻撃

図 6　周期性に着目した攻撃検知方式

Fig. 6　The attack detection method based on the periodicity.

3.　提案する攻撃方式の原理

3.1　攻撃手法の基本的なアイデアとその課題

攻撃を検知されないためには，正規の送信 ECU ではなりすましメッセージを受信できず，かつ受信 ECU では周期等から異常を検知されないようにする必要がある．すなわち，正規の送信 ECU の送受信を阻止し，かつ周期をなりすましたメッセージを注入することで，正規の送信 ECU および受信 ECU での異常検知ができなくなる．提案するなりすまし攻撃の基本アイデアとしては，**図 7** に示すように，正規の送信 ECU の送受信を阻止するためにバスオフ攻撃を行い，同時に，周期と CAN ID をなりすましたメッセージを注入する．しかしながら，この方法では以下に示す 2 つの課題が生じる．

課題 1．なりすましメッセージも正規メッセージと同じ CAN ID を持つためバスオフ攻撃の対象となり，なりすましメッセージ自体の送信も阻止されてしまう．

　対策として，攻撃者が送信中であることを検知し，バスオフ攻撃の対象から外す必要がある．

課題 2．正規の送信 ECU と攻撃者が同時に送信を開始したとき，ビットエラー誘発によるバスオフ攻撃が起こり，正規メッセージの送信を許す可能性がある．

攻撃者がエラーパッシブ状態で，かつ正規メッセージが攻撃者の送信するなりすましメッセージに対して，攻撃者をターゲット ECU で正規の送信 ECU を攻撃者として 2.2 節の条件 2. を満たすとき，同時送信時に正規メッセージの送信を許してしまう．同時に送信しないときにビットエラーが発生したときの波形図を**図 8** (a) に，同時に送信するときに正規メッセージが送信されるときの波形図を図 8 (b) に示す．図 8 (b) より，ビットエラーが発生した後，攻撃者がパッシブエラーフレームを送信するため，正規メッセージの送信を阻止することができない．なお，攻撃者も同時に送信しているため，ここで送信された正規メッセージは課題 1 の対策に従いバスオフ攻撃の対象とならず，バス上に送信されてしまう．

対策としては，何らかの方法で正規メッセージと攻撃者

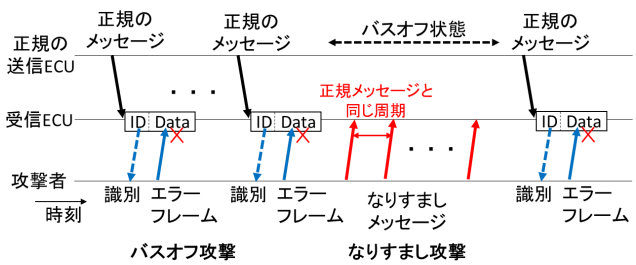
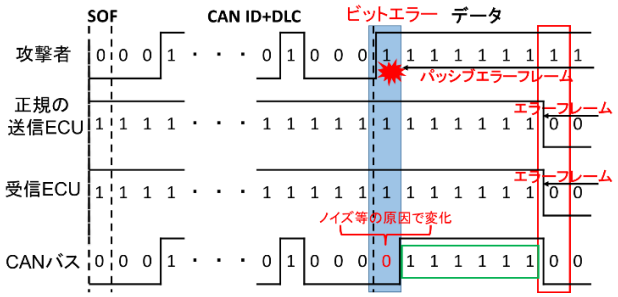
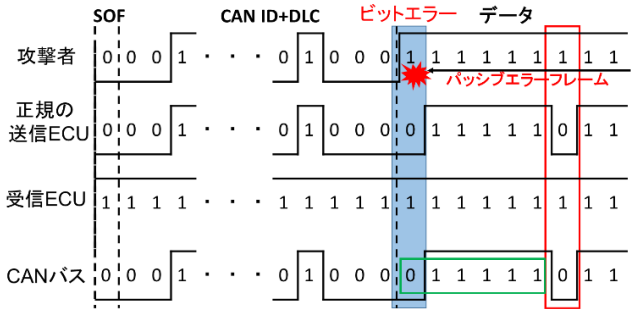


図 7　提案方式による攻撃の流れ

Fig. 7　The attack sequence of the proposed method.



(a) 通常時に起こり得るビットエラー時の波形



(b) ビットエラー誘発によるバスオフ攻撃時の波形

図 8　ビットエラー発生時の波形

Fig. 8　The waveform when a bit error occurs.

が送信したメッセージを識別する必要がある．

3.2　実装を意識した課題の解決方法

これらの課題を解決する方法として，CAN コントローラ内部の状態を取得して用いる方法と攻撃者の送信ビットおよび受信ビットを用いる方法が考えられる．CAN コントローラ内部の情報を利用する方法では，CAN コントローラを改造する必要があり，実装の難易度が上がる．本研究では攻撃者の送信ビットおよび受信ビットを用いる方法により課題 1 および課題 2 を解決する．ここで，送信ビットおよび受信ビットは CAN トランシーバにより電圧変換される前の値とする．以下では，課題 1 および課題 2 の解決策を，それぞれ解決策 1 および解決策 2 とする．

解決策 1．メッセージ送信時において，データフレーム中のドミナントに固定されているビットの受信時に攻撃者の送信ビットを確認する．送信ビットがドミナントであれば攻撃者が送信中であると判断し，バスオフ攻撃を行わない．

解決策 2．ビットエラー発生後に攻撃者の送信ビットと受信ビットを確認することにより，正規メッセージが送信されているかを確認する．もし，正規メッセージが送信されていれば，バスオフ攻撃を行う．具体的には，ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるときの直前 6 bit が同じ値でなければ，正規のメッセージが送信されていると判断し，バスオフ攻撃を行う．

メッセージを送信していない ECU はリセッシブのみを送信する．メッセージ送信中の ECU は送信する内容に合わせてリセッシブとドミナントを送信する．特に，データフレーム中のドミナントに固定されたビットにおいては必ずドミナントが送信される．ドミナントに固定されたビットの受信時において，攻撃者が送信していなければ攻撃者の送信ビットはリセッシブであり，送信していれば送信ビットはドミナントとなる．ゆえに，解決策 1 は有効である．本研究では，ドミナントに固定されたビットとして r0 ビットを用いる．

図 8 で例示された状況では，(A) 攻撃者と正規の送信 ECU が同時に送信していないとき，ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミングの直前 6 bit がすべて同じ論理を表すこと，および，(B) 攻撃者と正規の送信 ECU が同時に送信するとき，ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミングの直前 6 bit がすべて同じ論理ではないことの 2 つの条件が成り立つ．これらのことがつねに成り立つのであれば，解決策 2 が有効であることが確認できる．(1) では考慮する必要がある攻撃者と受信 ECU および正規の送信 ECU のエラー状態の組合せを確認し，(2) で攻撃者がビットエラーを検出した後に受信 ECU および正規の送信 ECU が検知するエラーの種類を確認する．(3) ではビットエラー発生後に初めて送信ビットと受信ビットが異なるタイミングを確認する．最後に，(1) と (2) と (3) の内容をふまえて，(A) と (B) がつねに成り立つことを示し，解決策 2 が有効であることを確認する．

(1) 攻撃者と受信 ECU および正規の送信 ECU のエラー状態

攻撃者と受信 ECU および正規の送信 ECU のエラー状態を検討する．攻撃者はメッセージを送信していることから，エラーアクティブ状態またはエラーパッシブ状態であることが分かる．攻撃者がエラーアクティブ状態であるとき，ビットエラー発生直後に攻撃者がアクティブエラーフレームを送信するため，正規メッセージがエラーにならずに送信を終えることはないため，攻撃者がエラーパッシブ状態であるときのみ検討する．受信 ECU および正規の送信 ECU については制約条件がないため，3 状態すべての場合が考えられる．

(2) 受信 ECU および正規の送信 ECU が検知するエラーの種類

メッセージ送信中の ECU がビットエラーを検出しエラーフレームを送信したとき，他の ECU が検出するエラーはフォームエラーかスタッフエラーである．ただし，(1) より攻撃者はエラーパッシブ状態であるため，固定フォーマットのビットフィールドを改ざんすることがなく，フォームビットエラーは発生しない．ビットエラー発生後にリセッシブを 6 bit 連続して受信したときに受信 ECU および正規の送信 ECU はスタッフエラーを検

出する．

(3) ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミング

攻撃者と正規の送信 ECU が同時に送信しないときと同時に送信するとき，ビットエラー発生後に初めて送信ビットと受信ビットが異なるタイミングを確認する．ただし，(2) の結果をふまえて，ビットエラー発生後に受信 ECU および正規の送信 ECU で発生するエラーはスタッフエラーのみであることを前提とする．

(3-1) 攻撃者と正規の送信 ECU が同時に送信しないとき

受信 ECU および正規の送信 ECU の中にエラーアクティブ状態の ECU が含まれるときと 1 台も含まれないときを分けて検討する．

(3-1-1) 受信 ECU または正規の送信 ECU がエラーアクティブ状態

ビットエラー発生後，攻撃者はパッシブエラーフレームすなわちつねにリセッシブを送信する．6 bit 連続してリセッシブが送信されるため，受信 ECU および正規の送信 ECU はスタッフエラーを検出し，直後にドミナントが含まれるアクティブエラーフレームを送信する．これより，スタッフエラーが発生した直後のビットがビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミングであることが確認できた．

(3-1-2) 受信 ECU と正規の送信 ECU のすべてがエラーパッシブ状態またはバスオフ状態

ビットエラー発生後，攻撃者はパッシブエラーフレームを送信する．受信 ECU と正規の送信 ECU はスタッフエラーを検出した直後にパッシブエラーフレームを送信するか，バスオフ状態であれば何も送信しない．これより，ビットエラー発生後に攻撃者の送信ビットと受信ビットが異ならないことが確認できた．

(3-2) 攻撃者と正規の送信 ECU が同時に送信するとき

ビットエラー発生後，攻撃者はパッシブエラーフレームを送信する．スタッフエラーが発生する前に，ビットスタッフィングルールにより必ず正規の送信 ECU がドミナントを送信し，正規メッセージの送信を続ける．これより，ビットエラー発生後に初めて正規メッセージにドミナントが含まれるときに攻撃者の送信ビットと受信ビットが異なることが確認できた．

(3) より，攻撃者と正規の送信 ECU が同時に送信していないとき，ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミングは受信 ECU および正規の送信 ECU がスタッフエラーを検出した直後のビットであることが分かった．スタッフエラーを検出していることから，このときの直前 6 bit はすべて同じ論理であり，(A) がつねに成り立つことが確認できた．攻撃者と正規の送信 ECU が同時に送信するとき，ビットエラー発生後に初めて攻撃者の送信ビットと受信ビットが異なるタイミングはビットエラー発生後に初めて正規メッセージにドミナントが含まれるときであることが分かった．ビットスタッフィングルールより，このときの直前 6 bit がすべて同じ論理になることはないため，(B) がつねに成り立つ．以上より，ビットエラー発生後，最初に攻撃者の送信ビットと受信ビットが異なるときの直前 6 bit が同じ値でなければ，正規のメッセージが送信されていると判断することができる．すなわち，解決策 2 が有効であることが確認できた．

3.3　提案方式の攻撃アルゴリズム

実装を意識した提案方式の攻撃アルゴリズムの詳細を説明する．アルゴリズムは (1) メッセージ受信時と，(2) なりすましメッセージ送信と，(3) なりすましメッセージ送信中に攻撃者の送信ビットと受信ビットが異なったときと，(4) バスアイドルを検知したときに分けられる．

(1) メッセージ受信時のアルゴリズムを以下に示す．

1. データフレームの CAN ID 部を受信した後，攻撃対象の CAN ID であるかを確認する．
2. 1. で確認した CAN ID が攻撃対象であればバスオフ攻撃を行い，正規の送信 ECU を無効化する．

(2) なりすましメッセージ送信時のアルゴリズムを以下に示す．

1. CAN ID と周期をなりすましたメッセージを送信する．

(3) なりすましメッセージ送信中に攻撃者の送信ビットと受信ビットが異なったときのアルゴリズムを以下に示す．

1. フラグが立っていれば 1.1 へ立っていなければ 1.2 へ．
   - 1.1 直前 6 bit を確認して，すべて同じ論理値であれば 3. へ，すべて同じ論理値でなければ 2. へ．
   - 1.2 フラグを立てて，3. へ．
2. バスオフ攻撃を行い，正規の送信 ECU を無効化する．
3. 1 bit 期間待機し，攻撃者の送信ビットと受信ビットの監視に戻る．

(4) バスアイドルを検知したときのアルゴリズムを以下に示す．

1. フラグを下げる．

以上が提案する攻撃方式のアルゴリズムである．このアルゴリズムに従い攻撃を行うことで，従来の方式で検知されない攻撃が実現する．

3.4　提案方式が適用可能な条件

提案した攻撃方式はバスオフ攻撃などの CAN の規格に

準拠していない特別な機能が必要となる．そのため，提案した攻撃方式を実装した専用のハードウェアを CAN バスに直接接続する必要がある．CAN バス上であれば接続箇所に制約はないため，車内に侵入し OBD-II ポートや内部の CAN バス上の任意の箇所に接続することで攻撃が可能となる．

CAN の規格ではバスオフ状態からエラーアクティブ状態に遷移する条件として，バス上に連続した 11 bit のリセッシブビットを 128 回検出する必要があるとされている．しかし，規格に従わずバスオフ状態に遷移した後に即時エラーアクティブ状態に遷移する ECU も存在する．提案方式は特別な改造をされた CAN コントローラを用いた ECU は対象としていないため，そのような ECU に対しては有効でない場合もありうる．

4. 評価実験

4.1 実験環境と評価項目

本研究では，提案方式の実現可能性を示すために，FPGA（Field Programmable Gate Array）とマイクロコントローラを用いて攻撃装置を実装した．**図 9** の構成図におけるバスオフ攻撃部は FPGA を用いて実装し，なりすまし攻撃部はマイクロコントローラ上のソフトウェアとして実装した．攻撃装置を構築するのに以下の 4 つのデバイスを用いた．

1. FPGA ボード（ZedBoard）
2. SPI 通信可能なマイクロコントローラ（ATmega328P）
3. CAN コントローラ（MCP2515）
4. CAN トランシーバ（MCP2551）

図 10 に実験で用いる模擬環境を示す．攻撃装置と正規の送信 ECU と受信 ECU と CAN バス解析ツールを 1 つの CAN バスにすべて接続した．また，CAN バスの観測のために，CAN バス解析ツールである Vehicle Spy3 を用いる．CAN 通信は一般的な車載環境と同じ 500 Kbps に設定した．なりすまし対象のメッセージは CAN ID が 1C4 で周期が 23 ms のメッセージとした．正規の送信メッセージのデータは “00 00 00 00 00 00 00 00” で，なりすましメッセージのデータを “17 70 00 00 00 00 00 00” とした．実車での実験には国産ハイブリッド自動車を用いた．実車での実験においても模擬環境での実験と同じメッセージを用いた．特に，実験に利用した車種において，CAN ID が 1C4 のメッセージはエンジンの回転数を表す．

本研究では，正規の送信 ECU でなりすましメッセージを受信できず，受信 ECU で周期から異常を検知できない攻撃の実現可能性の評価を目的としている．そこで，提案方式の評価項目として，以下の 3 つをあげる．

評価項目 1．なりすましメッセージの割合

評価項目 2．正規の送信 ECU で受信したなりすましメッセージ数

評価項目 3．攻撃時における，周期の変化

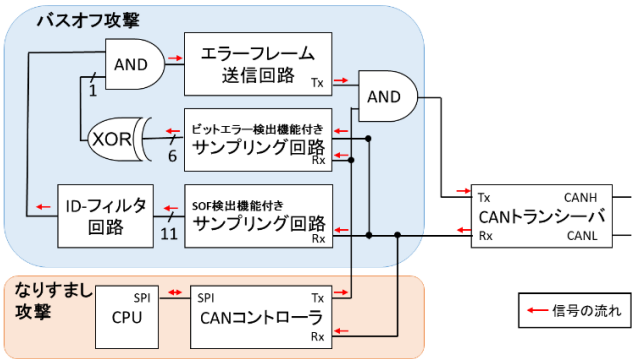


図 9　攻撃装置の構成

Fig. 9　The configuration of the attack device.

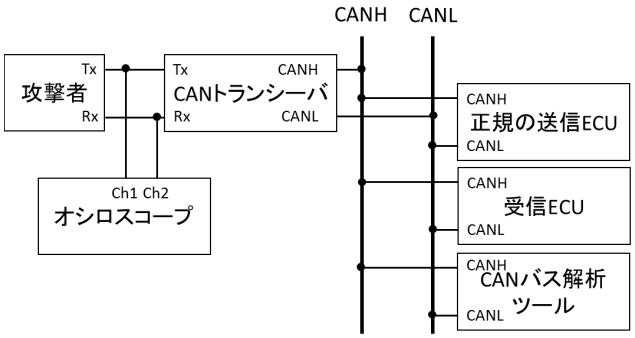


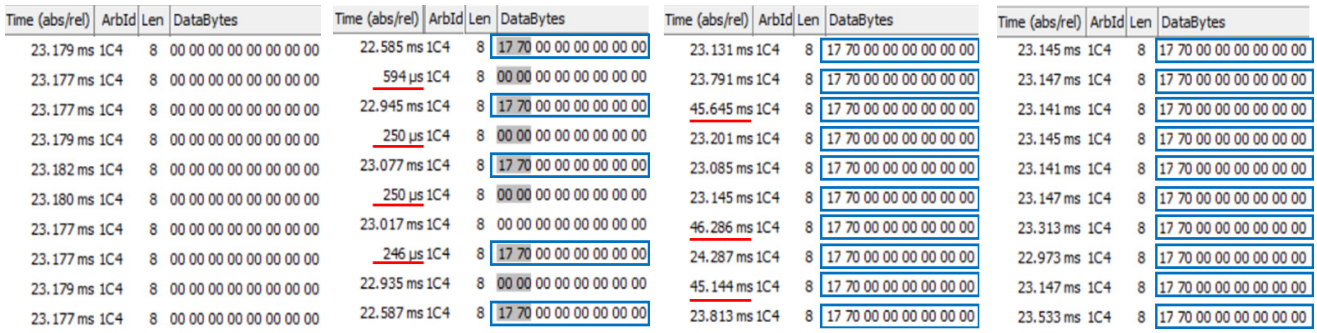
図 10　模擬環境での実験構成

Fig. 10　The experimental configuration of the simulated environment.

評価項目 1 では，CAN バスに送信された攻撃対象の CAN ID を持つメッセージのうちなりすましメッセージの割合を評価する．割合が低くなるほど，正規メッセージとなりすましメッセージが入り乱れることになるため，異常検知される可能性が高くなる．評価項目 2 では，正規の送信 ECU で受信できたなりすましメッセージの数を評価する．正規の送信 ECU では自身が送信したメッセージと他から送信されたなりすましメッセージを区別できるため，なりすましメッセージを受信できると異常検知が可能となる．評価項目 3 では，通常時と攻撃時の周期を比較する．受信 ECU では周期から異常を検知するため，攻撃時に周期が大きく変化するだけ，異常検知される可能性が高くなる．

4.2 模擬環境での実験結果

4.1 節で示した模擬環境上で，周期をなりすましたメッセージを注入する方式と提案方式を用いて評価実験を行う．本研究では，提案方式に用いるバスオフ攻撃として，スタッフエラー注入によるバスオフ攻撃と 1 フレームでのバスオフ攻撃を用いる．今回，メッセージの割合を調べるため，攻撃開始後，攻撃者は周期に合わせて 100 回なりすましメッセージの送信命令を CAN コントローラに送るもの



(a)　通常時　(b) 周期をなりすましたメッセージを注入する方式　(c) スタッフエラー注入によるバスオフ攻撃を利用した方式　(d) 1 フレームでのバスオフ攻撃を利用した方式

図 11　各方式におけるなりすましメッセージの割合と周期の比較

Fig. 11　The comparison of the ratio of spoofing messages and the period.

表 2　なりすましメッセージの割合

Table 2　The ratio of spoofing messages.

方式	割合
周期をなりすましたメッセージを注入する方式	50%
スタッフエラー注入によるバスオフ攻撃を利用した方式	100%
1 フレームでのバスオフ攻撃を利用した方式	100%

表 3　正規の送信 ECU で受信したメッセージ数

Table 3　The number of messages received by the regular transmission ECU.

	正規の送信 ECU における受信メッセージ数	攻撃者における送信メッセージ数
周期をなりすましたメッセージを注入する方式	100	100
スタッフエラー注入によるバスオフ攻撃を利用した方式	36	93
1 フレームでのバスオフ攻撃を利用した方式	0	100

とした．実験結果における一例を**図 11** に示す．図 11 (a) は通常時であり，図 11 (b) と図 11 (c) と図 11 (d) は各方式による攻撃時の結果である．赤の下線は通常時に比べて周期が変化していることを表し，青枠はなりすましメッセージを表す．周期をなりすましたメッセージを注入する方式に限り，正規メッセージが送信されていた．1 フレームでのバスオフ攻撃を利用した方式は，比較的周期の変動が少なかった．

評価項目 1 について，実験より得られた結果を**表 2** に示す．実験結果より，周期をなりすましたメッセージを注入する方式では正規メッセージとなりすましメッセージが同じ割合で送信されていることが分かる．また，提案方式ではなりすましメッセージの割合が 100%となっており，正規メッセージの送信を確実に阻止していることが分かる．

評価項目 2 について，実験より得られた結果を**表 3** に示す．実験結果より，周期をなりすましたメッセージを注入する方式では，正規の送信 ECU がすべてのなりすましメッセージを受信していることが分かる．また，スタッフエラー注入によるバスオフ攻撃を利用した方式では，100 回なりすましメッセージの送信命令を行ったにもかかわらず 93 回しかメッセージが送信されなかった．さらに，93 メッセージ中 36 メッセージは正規の送信 ECU に受信されていた．1 フレームでのバスオフ攻撃を用いたときは，100 メッセージすべてが送信され，正規の送信 ECU に受信されることはなかった．

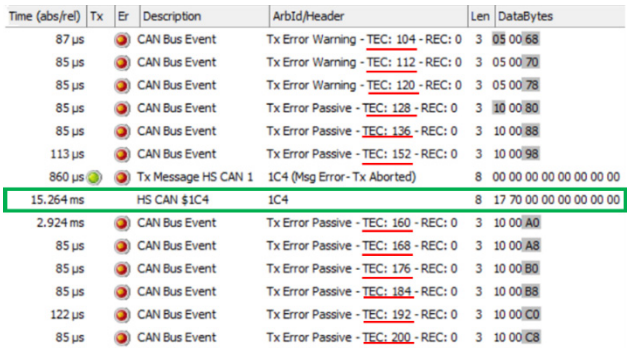
表 4　攻撃における周期の変化

Table 4　The changes of the period in attack.

方式	最短[ms]	最長[ms]	平均[ms]
通常時	23.17	23.19	23.18
周期をなりすましたメッセージを注入する方式	0.25	23.09	12.75
スタッフエラー注入によるバスオフ攻撃を利用した方式	18.57	46.29	30.34
1 フレームでのバスオフ攻撃を利用した方式	22.57	23.71	23.14

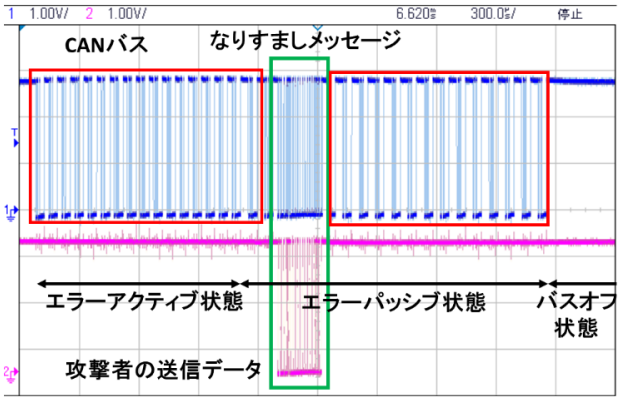
評価項目 3 について，実験より得られた結果を**表 4** に示す．通常時は周期の平均が 23.18 ms で，周期の変動幅は 0.02 ms すなわち周期の 0.1%程度となった．周期をなりすましたメッセージを注入する方式では，周期の平均が通常時の約半分の長さで，変動幅は約 1 周期の長さとなった．スタッフエラー注入によるバスオフ攻撃を利用した方式は，周期の平均が通常時より約 7 ms 程度長く，変動幅は 1 周期以上の長さとなった．1 フレームでのバスオフ攻撃を利用した方式は，周期の平均が通常時に比べて 0.2%程度短くなり，変動幅は周期の 5%以下となった．

スタッフエラー注入によるバスオフ攻撃を利用した方式での攻撃時に，100 回なりすましメッセージの送信命令を行ったにもかかわらず 93 回しかメッセージが送信されなかったことの原因を確認するために追実験を行った．追実験では，攻撃中における攻撃者の TEC と状態を確認したところ，攻撃中に TEC が増加してバスオフ状態に遷移した．同様に，正規の送信 ECU がなりすましメッセージを受信した原因を確認するために追実験を行った．追実験では，正規の送信 ECU の代わりに CAN バス解析ツールである Vehicle Spy3 のメッセージ送信機能を用いた．**図 12**



Time (abs/rel)	Tx	Er	Description	ArbId/Header	Len	DataBytes
87 µs			CAN Bus Event	Tx Error Warning - TEC: 104 - REC: 0	3	05 00 68
85 µs			CAN Bus Event	Tx Error Warning - TEC: 112 - REC: 0	3	05 00 70
85 µs			CAN Bus Event	Tx Error Warning - TEC: 120 - REC: 0	3	05 00 78
85 µs			CAN Bus Event	Tx Error Passive - TEC: 128 - REC: 0	3	10 00 80
85 µs			CAN Bus Event	Tx Error Passive - TEC: 136 - REC: 0	3	10 00 88
113 µs			CAN Bus Event	Tx Error Passive - TEC: 152 - REC: 0	3	10 00 98
860 µs			Tx Message HS CAN 1	1C4 (Msg Error - Tx Aborted)	8	00 00 00 00 00 00 00 00
15.264 ms			HS CAN $1C4	1C4	8	17 70 00 00 00 00 00 00
2.924 ms			CAN Bus Event	Tx Error Passive - TEC: 160 - REC: 0	3	10 00 A0
85 µs			CAN Bus Event	Tx Error Passive - TEC: 168 - REC: 0	3	10 00 A8
85 µs			CAN Bus Event	Tx Error Passive - TEC: 176 - REC: 0	3	10 00 B0
85 µs			CAN Bus Event	Tx Error Passive - TEC: 184 - REC: 0	3	10 00 B8
122 µs			CAN Bus Event	Tx Error Passive - TEC: 192 - REC: 0	3	10 00 C0
85 µs			CAN Bus Event	Tx Error Passive - TEC: 200 - REC: 0	3	10 00 C8

(a) CAN バス解析ツールによる送受信記録



(b) オシロスコープによる CAN バスと攻撃者の送信データ

図 12　バスオフ攻撃中に送信されたなりすましメッセージ

Fig. 12　The spoofed messages transmitted on the bus-off attack.

は，バスオフ攻撃により正規の送信 ECU が連続して送信エラーになっていることと，バスオフ攻撃中になりすましメッセージが送信されていることを表している．緑枠に囲まれているメッセージがなりすましメッセージである．図 12 (a) より，正規の送信 ECU がなりすましメッセージを受信したときには，TEC が 152 すなわち正規の送信 ECU がすでにエラーパッシブ状態であることが分かる．図 12 (b) は，CAN バス上に流れているデータと攻撃者が送信したデータを表す波形である．この図の赤枠で囲まれている波形は連続してエラーになっていることを表し，緑枠はなりすましメッセージを送信していることを表す．この図からも正規の送信 ECU がエラーパッシブ状態であることが分かる．以上より，正規の送信 ECU がエラーパッシブ状態であるときに，攻撃者がなりすましメッセージを送信しているため，正規の送信 ECU がなりすましメッセージを受信した．

4.3　実車での実験結果

なりすまし対象はエンジン回転数とし，アイドリングストップ時になりすまし攻撃を行うことで不正な値を表示させる．なお，周期をなりすましたメッセージを注入する方式では正規の 0 rpm を表すメッセージと競合することから，タコメータの指針は 0 となりすました値の間でふらつく．そのため，完全になりすました値になることはない．目視でのふらつきを止めるには，実験に用いた自動車の場合，通常の周期に対して約 50 倍のなりすましメッセージを注入する必要があった [4]．一方，提案方式では，正規メッセージの送信が阻止されていることにより，通常の周期でなりすましメッセージを注入するだけで十分であった．

表 5　攻撃における周期の変化

Table 5　The changes of the period in attack.

方式	最短[ms]	最長[ms]	平均[ms]
通常時	22.70	24.10	23.55
1 フレームでのバスオフ攻撃を利用した方式	22.91	24.04	23.48

模擬環境での実験で結果が最も優れていた 1 フレームでのバスオフ攻撃を利用した方式でのなりすまし攻撃を実施した．結果として，エンジン停止中であるにもかかわらず，タコメータの指針がなりすました値を指し，ふらつくこともなかった．実験に使った自動車において，攻撃中にエラー表示が出ることもなかった．評価項目 1 については，同様になりすましメッセージの割合が 100%となった．評価項目 2 については正規の ECU で受信したメッセージを確認する手段がないため，確認することはできなかった．評価項目 3 について，実験より得られた結果を**表 5** に示す．通常時に比べて，攻撃時の平均は周期の 0.5%程度短くなった．周期が通常時の最短 < 攻撃時の最短，かつ攻撃時の最長 < 通常時の最長の関係にあるため，周期に着目した攻撃検知方式で正規メッセージを誤検知しないように許容範囲を設定すると，攻撃を検知することはできない．

5.　考察

本章では，模擬環境での各方式における実験結果と実車実験での実験結果より考察を行い，提案方式が新たな脅威になるかを総合的に判断する．

周期をなりすましたメッセージを注入する方式では，評価項目 1 に関する実験より，正規メッセージとなりすましメッセージが同じ割合で CAN バスに送信されることが分かった．これは，正規の送信 ECU の送信を阻止していないためである．評価項目 2 に関する実験より，正規の送信 ECU の受信を阻止していないため，正規の送信 ECU ですべてのなりすましメッセージを受信した．評価項目 3 に関する実験より，攻撃時における周期の変動幅が最大で 1 周期以上で，送信周期に対する平均遅延が 7 ms 程度発生していることが分かった．以上より，周期をなりすましたメッセージを注入する方式では，正規の送信 ECU および受信 ECU で攻撃を検知される可能性が高い．

スタッフエラー注入によるバスオフ攻撃を利用した方式では，評価項目 1 に関する実験より，なりすましメッセージのみ CAN バスに送信されることが分かった．これは，正規の送信 ECU の送信を阻止しているからである．

評価項目 2 に関する実験より，正規の送信 ECU で 93 メッセージ中の 36 メッセージを受信した．追実験より，正規の送信 ECU がエラーパッシブ状態であるときになりすましメッセージを注入したためであることが分かった．100 回なりすましメッセージの送信命令をしたにもかかわらず 93 メッセージしか送信されなかった原因は，攻撃中に攻撃者がバスオフ状態に遷移して送信を止めるためであると考えられる．具体的には，正規メッセージとなりすましメッセージが同時に送信されたとき，ビットエラーが発生するため，攻撃者 ECU のエラーカウント値が増加する．これにより，攻撃者がバスオフ状態に遷移し，なりすましメッセージの送信を中止するためである．評価項目 3 に関する実験より，周期の変動幅が最大で 1 周期以上で，送信周期に対する平均遅延が 7 ms 程度発生していることが分かった．正規メッセージとなりすましメッセージが同時に送信されたとき，攻撃者がバスオフ状態に遷移してなりすましメッセージの送信を中止する可能性がある．このとき，次のなりすましメッセージの送信まで 1 周期の待機時間が発生するため，最大で 1 周期以上の遅延が発生したと考えられる．送信周期に変動があるのは，正規の送信 ECU がバスオフ攻撃を受けているときに，正規の送信 ECU がエラーパッシブ状態に遷移するまで，送信を待機する必要があるからであると考えられる．以上より，スタッフエラー注入によるバスオフ攻撃を利用した方式では，正規の送信 ECU および受信 ECU で攻撃を検知される可能性が高い．

1 フレームでのバスオフ攻撃を利用した方式では，評価項目 1 に関する実験より，スタッフエラー注入によるバスオフ攻撃を利用した方式と同様に，なりすましメッセージのみ CAN バスに送信されることが分かった．評価項目 2 に関する実験より，正規の送信 ECU でなりすましメッセージを受信することはなかった．評価項目 3 に関する実験より，変動幅が周期の 5%以下となった．通常時は 0.1%程度であったため，50 倍近くになっている．今回の実験では，正規の送信 ECU は正規メッセージのみを送信する機能だけであったため，処理による遅延が小さく，通常時の変動幅が短かったと考えられる．文献 [8] で提案されている周期性に着目した方式では，許容範囲を周期の 80%程度まで広げていないと，正常時に攻撃と判断する誤検知が発生していた．これより，変動幅が周期の 5%程度であれば，周期に着目した攻撃検知方式で検知される可能性が低いと考えられる．しかし，文献 [16] で提案されている方式では，設計段階で計算された最大遅延時間を用いることにより，前述の方式より厳密に周期を監視している．本文献では最大遅延時間として具体的な数値が明記されていないため比較はできないが，前述の方式に比べて検知できる可能性が高くなると考えられる．以上より，1 フレームでのバスオフ攻撃を利用した方式では，CAN の規格に準拠した正規の送信 ECU での検知は難しく，受信 ECU においても最大遅延時間などの事前知識なく検知する方式で検知することは難しいと考えられる．

正規の送信 ECU がなりすましメッセージを受信した原因を確認するために行った追実験の実験結果である図 12 (a) より，正規の送信 ECU がパッシブエラー状態に遷移してすぐにエラーアクティブ状態である攻撃者がなりすましメッセージを送信できていないことが分かる．バスオフ攻撃時において，正規の送信 ECU がエラーアクティブ状態である間になりすましメッセージが攻撃者 ECU の送信バッファに溜まっていれば，正規の送信 ECU がエラーパッシブ状態に遷移した直後になりすましメッセージが送信される．図 12 (a) では，遅れて送信されていることから，正規の送信 ECU がエラーパッシブ状態に遷移した後になりすましメッセージが攻撃者 ECU の送信バッファに溜まったことが分かる．

模擬環境の実験では攻撃時における周期の変動幅が通常時より大きくなったが，実車実験では攻撃時における周期の変動幅が通常時より小さくなった．これは実車の ECU ではメッセージ送信以外の処理も行うため，遅延が発生したことが原因と考えられる．評価項目 2 に関しては確認を行うことができなかったが，他の評価項目においては模擬環境での実験結果と比較して，同等もしくは良好な結果が得られた．以上より，提案方式は新たな脅威といえる．

6. おわりに

本研究では，バスオフを用いて正規の送信 ECU の送受信を阻止し，周期をなりすましたメッセージを注入することで，正規の送信 ECU および受信 ECU でも検知できない攻撃を提案した．提案方式を FPGA とマイクロコントローラにより実装し，模擬環境と実車で評価実験を行った．実験結果より，1 フレームでのバスオフ攻撃を用いることで，正規の送信 ECU および受信 ECU で検知できない攻撃が実現可能であることを示した．今後の課題として，提案方式は CAN における新たな脅威として考え，提案方式も検知できる方式を検討する必要がある．

参考文献

[1] International Organization for Standardization: Road vehicles, controller area network (CAN), Part 1: Data link layer and physical signaling, ISO IS11898-1 (2015).
[2] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S.: Experimental Security Analysis of a Modern Automobile, *Proc. 2010 IEEE Symposium on Security and Privacy*, pp.447–462 (May 2010).
[3] Miller, C. and Valasek, C.: Remote Exploitation of an Unaltered Passenger Vehicle, *Black Hat USA 2015*, pp.1–91 (Aug. 2015).
[4] Ezaki, T., Date, T. and Inoue, H.: An Analysis Platform for the Information Security of In-vehicle Networks Con-

nected with the External Networks, *Proc. 10th International Workshop on Security*, pp.301–315 (Aug. 2015).
[5] 倉地　亮，松原　豊，高田広章，上田浩史，堀端啓史：メッセージ認証を用いたCANの集中監視システム，電子情報通信学会論文誌 A，Vol.J99-A, No.2, pp.118–130 (2016).
[6] 中野将志，久保田貴也，汐崎　充，藤野　毅：車載CAN通信の暗号化とリプレイ攻撃対策手法の実装評価，情報処理学会研究報告 EMB，Vol.36, No.2, pp.1–6 (Feb. 2015).
[7] Dariz, L., Selvatici, M., Ruggeri, M., Costantino, G. and Martinelli, F.: Trade-off analysis of safety and security in CAN bus communication, *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems* (*MT-ITS*), pp.226–231 (June 2017).
[8] 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，*SCIS2017*, pp.1–8 (Jan. 2017).
[9] Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K. and Oishi, K.: A method of preventing unauthorized data transmission in controller area network, *IEEE Vehicular Technology Conference* (2012).
[10] Cho, K. and Shin, K.G.: Error Handling of In-vehicle Networks Makes Them Vulnerable, *Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security* (*CCS2016*), pp.1044–1055 (Oct. 2016).
[11] 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，*SCIS2017*, pp.1–8 (Jan. 2017).
[12] 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，*SCIS2015*, pp.1–8 (Jan. 2015).
[13] 菅原　健，佐伯　稔，三澤　学：強いリセッシブを用いたCANの電気的データ改ざん，電子情報通信学会技術研究報告 ICSS，Vol.114, No.489, pp.67–72 (Feb. 2015).
[14] 岸川　剛，松島秀樹，芳賀智之，前田　学，海上勇二，氏家良浩：車載ネットワークシステム，不正検知電子制御ユニット及び不正対処方法，国際特許 公開番号 WO2015/170451 (2015).
[15] 倉地　亮，高田広章，上田浩史，堀端啓史：CANにおけるエラーフレーム監視機構の提案，*CSS2015*, pp.110–115 (Oct. 2015).
[16] 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，*SCIS2015*, pp.1–7 (Jan. 2015).

推薦文

本論文は，バスオフ攻撃を用いたECU通信の阻止，およびメッセージ送信の工夫による，新たななりすまし攻撃による威嚇を提案しています．また，FPGAを用いた実験による信頼性の高い検証を行っています．これらは，将来の社会インフラとして期待の高い自動車制御システムの安全性実現に向けた，優れた情報提供であると思います．

（コンシューマ・デバイス&システム研究会主査　寺島美昭）

家平 和輝　（ジュニア会員）

2015年より広島市立大学情報科学部情報工学科．他に，セキュリティ・キャンプ全国大会2017修了，いちだいプログラミング教室実行委員会代表等．自動車の情報セキュリティについての脆弱性や防御機構の研究開発およびICT教育に従事．DICOMO2017優秀論文賞受賞．

井上 博之　（正会員）

1987年大阪大学工学部電子工学科卒業．1989年大阪大学大学院工学研究科電子工学専攻修了．1989年～2000年住友電気工業株式会社．1998年奈良先端科学技術大学院大学情報科学研究科博士後期課程単位取得退学，博士（工学）．2000年～2007年株式会社インターネット総合研究所および株式会社IRIユビテック．2007年より広島市立大学大学院情報科学研究科．現在は同大学准教授．他に，一般社団法人重要生活機器連携セキュリティ協議会研究開発センターチーフ，SECCON実行委員，SecHack365実行委員，セキュリティ・キャンプ全国大会講師等．広域ネットワークにつながる家電や自動車の情報セキュリティについて，その脆弱性やセキュアな通信プロトコルに関する研究開発に従事．電子情報通信学会，IEEE各会員．

石田 賢治　（正会員）

1989年広島大学大学院工学研究科博士課程後期了．同年広島県立大学講師．同大学助教授を経て，1997年から広島市立大学情報科学部助教授．2003年より同大学情報科学部教授．工学博士．ネットワーク制御アルゴリズム，アシュアランスシステムに関する研究に従事．1998年，2000年，2012年，2015年電子情報通信学会情報ネットワーク研究賞受賞．IEEE，ACM，電子情報通信学会各会員．