Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

先進運転支援システムを搭載した自動車に対する制御乗っ取り攻撃の脅威分析

中野将志[†1]　久保田貴也[†2]　汐崎充[†2]　藤野毅[†3]

概要：近年，自動車の高度な電子化，ネットワーク化が進展しており，それにともない，車載ネットワークの脆弱性をついた自動車制御の乗っ取り事例などが報告されるようになってきている．このような攻撃の脅威に対しては，メッセージの送信周期などに着目し不正なメッセージを打ち落とす対策や，メッセージ認証コード（MAC）を付加することでなりすましを阻止する対策など様々な対策が提案されている．本稿では，近年になって自動車への搭載が急速に進んでいる先進運転支援システム（ADAS）の脆弱性について調査した結果を報告する．実験に用いた自動車では，ADAS-ECU になりすました ODB-II ポートからのメッセージで自動ブレーキを作動させる攻撃が容易に行えることがわかった．また，自動ブレーキのような緊急回避動作時は，通常の送信周期から外れるメッセージが存在するため，メッセージの送信周期に着目した対策手法を適用することは困難だと考えられる．そこで，本稿では現状の CAN のメッセージに使用されているチェックサムフィールドを活用した軽量 MAC 認証手法を紹介し，少ないペイロード負荷で不正メッセージに対する堅牢性を備えることができることを示す．また，軽量 MAC 認証手法特有のリプレイ攻撃に対する検討結果についても述べる．

キーワード：自動車セキュリティ，Controller Area Network（CAN），先進運転支援システム（ADAS）

Threat analysis of spoofing attacks on vehicles equipped with the Advanced Driving Assistant System

MASASHI NAKANO[†1]　TAKAYA KUBOTA[†2]　MITSURU SHIOZAKI[†2]
TAKESHI FUJINO[†3]

Abstract: Along with the progress of connected vehicles, cyber-attacks exploiting the vulnerability of vehicle network have been reported in research papers. Against threat of such attacks, there have been proposed various countermeasures such as disturbing the malicious message by utilizing the transmission period, or invalidating the received message by checking the Message Authentication Code (MAC). In this paper, we studied the vulnerability of Advanced Driving Assistant System (ADAS) mounted on recent vehicles. In our experiment, the emergency braking operation is easily activated by the spoofing message as an ADAS-ECU from the ODB-II port. The previously proposed countermeasures utilizing the message transmission period is difficult to apply in the emergency situation, because the control-message-interval deviate from the normal transmission cycle. Therefore, we have proposed a lightweight MAC authentication technique utilizing the checksum field used in current state of the CAN messages, indicating that the robustness is kept on the emergency situation with a small increase of payload. In addition, we investigated the possibility of replay attack on our lightweight MAC authentication method.

Keywords: Embedded security, Controller Area Network（CAN）, Advanced Driving Assistant System（ADAS）

1. はじめに

近年，運転支援システムや自動運転システムに見られるように自動車の高度な電子化・ネットワーク化が進展している．更に，Intelligent Transport Systems（ITS：高度交通システム）では車車間通信や路車間通信，さらにはインターネットと情報をやり取りしながら，渋滞の回避や快適な運転など自動車の利便性や安全性の向上を目指した取り組みがなされている．一方で，このように自動車が様々な機器やネットワークに繋がることによりサイバー攻撃の対象となる可能性が高まってきた．中でも，車載組込みシステムに数多く搭載している Electronic Control Unit（ECU）と呼ばれる制御マイコンを狙った自動車乗っ取りの事例がいくつか報告されている．よく知られているのは，2010 年に Kohno らによって本来自動車の保守に使用する On-Board Diagnostics 2nd edition（OBD-II）ポートから Controller Area Network（CAN）経由で ECU へ侵入することができる自動車セキュリティの問題点を指摘した報告である[1]．また，2013 年には OBD-II ポートから CAN に不正なメッセージを送信することでステアリングやブレーキなどの不正操作が実際に成功する事例が報告されている[2]．日本の研究会でも，OBD-II ポートに携帯回線を接続し，自動車のインストルメントパネル不正表示やボディ系なりすまし制御を実行するという報告が行われた[3]．更に 2015 年にはインターネット経由での遠隔操作が実証[4]され，自動車メーカーがリコールを発表するといったことも起きている．このよう

†1 立命館大学大学院理工学研究科
Graduate School of Science and Technology, Ritsumeikan University
†2 立命館大学大学院総合科学技術研究機構,
Research Organization of Science and Engineering, Ritsumeikan University
†3 立命館大学理工学部
Department of Science and Engineering, Ritsumeikan University

Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

な車載システムのセキュリティは財産的価値に留まらず，人命にも関わる大きな問題となるため，対策技術が重要な課題である．

現在，対策としては，インターネット回線などの外部からの侵入に対してセキュリティゲートウェイを設置するネットワークセキュリティ技術の適用，車載ネットワーク内に対してエンジン，ブレーキ，ステアリングといった“安全に直結する重要な制御情報”には Message Authentication Code（MAC）を用いたメッセージ認証を行うことで改ざん検知を行う対策[5][6]や，通信メッセージを監視して不正なメッセージを検知する対策[7] [8][9]が議論されている．

本論文では，まず近年になって急速に搭載が進んでいる先進運転支援システム（ADAS：Advanced Driving Assistant System）の脆弱性について調査した結果を示す．中でも，この先進運転支援システムは自動車がより能動的に制御を行う安全技術であるため，その制御に対する攻撃が脅威と成り得ないかといった点に注目した．また，自動ブレーキのような緊急回避動作時には，通常の送信周期から外れるメッセージが存在していることがわかったため，通信メッセージを監視・検知する対策が先進運転支援システムにおいても有効かを考察する．そして，我々が攻撃対策として提案した軽量 MAC 認証手法[10]の有効性やリプレイ攻撃対策について検討した結果を報告する．

以降，第 2 章では車載ネットワークの問題点と既存の対策手法について述べ，第 3 章では先進運転支援システムをターゲットとして，不正メッセージによるブレーキ制御乗っ取り攻撃を行った実験結果を示す．第 4 章では軽量 MAC 認証手法のリプレイ攻撃対策について述べる．最後に，第 5 章で全体のまとめと今後の課題について記述する．

2. 車載ネットワークの問題点と既存対策

2.1 車載ネットワークの問題点

現在の自動車内のネットワークでは，代表的な通信プロトコルとして CAN[11]が普及している．CAN は，ISO15118 で標準化された通信プロトコルである．CAN 通信のイメージを図 1 に，その特徴を表 1 に示す．メッセージを送信する ECU は，送信 ID を付けてメッセージをブロードキャストで送信する．受信する ECU は，受信 ID と一致した場合メッセージを受信することができる．またメッセージには，最大 8Byte のデータを格納して送信することができる．

CAN 通信のセキュリティ上の問題点は 2 点ある．1 つは，ブロードキャスト型のプロトコルで通信しているため通信線に接続することができれば，誰でもメッセージを受信することができ，盗聴が容易という点である．また，暗号化も行われていないため，メッセージの解析も容易である．もう 1 つは，通信相手の認証プロセスがないため，悪意を持った送信者に不正なメッセージを送信されると，誤ったデータを受け取ってしまう危険性がある点である．このように現在の CAN 通信は，セキュリティに対して考慮がなされていないため，攻撃者が車載診断用の OBD-II ポート経由に不正なメッセージを送信，不正 ECU の装着，正規 ECU の不正書き換え等を行うことにより表 2 に示すような脅威が問題となる．これらの脅威の中でも，なりすまし攻撃やリプレイ攻撃は ECU の制御が乗っ取られることで自動車の走行を危険な状態にする可能性があるため対策が必要である．

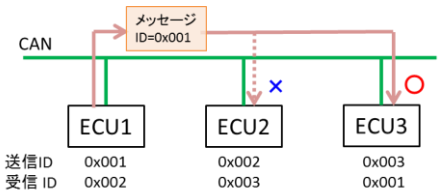

図 1　CAN 通信のイメージ

表 1　CAN 通信の特徴

特徴	説明
バストポロジ	1つの通信線に複数のECUを接続.
CSMA方式（Carrier Sense Multiple Access）	バスが空いていれば，すべてのECUがメッセージを送信できる. ECUの動的な追加・離脱が可能.
送信権の調停	同時にデータが送信された場合，CAN-IDを用いた送信権の調停を行う．優先度の高いメッセージが優先的に送信され，優先度の低いメッセージは優先度の高いメッセージの送信が完了してから送信される.

表 2　CAN 通信への攻撃

脅威	説明
盗聴・解析	メッセージを不正に取得し，内容の解析を行う.
なりすまし攻撃	特定のECUに対して，偽のメッセージを送り，制御の乗っ取りを行う.
リプレイ攻撃	正常な通信メッセージを記録し，同じようにメッセージを送ることで，制御の乗っ取りを行う.

2.2 既存の対策手法とその課題

前述した脅威に対して，幾つか対策手法が提案されている．それらは 1) 通信を監視して不正なメッセージの存在を検知する手法と，2) メッセージ認証により通信データの改ざん検知をし，完全性を保証する手法に分けられる．

不正なメッセージの存在を検知する手法には，通常時よりもメッセージが多く通信されている異常を検知する[7]，周期的にメッセージが送信されることを利用して検知する[7][8]などが提案されている．また，メッセージの ID，データ長，送信周期，送信頻度などに加え，データの変化量や範囲なども監視することで不正メッセージを検出する多層連携 CAN フィルタ[9]も提案されている．しかしながら，これらの手法では，走行中の状況毎に通信メッセージが不正か否かを正確に判断されることが求められ，その精度や適用範囲を考慮していくとシステムが複雑化していくと予想される．

一方で，メッセージ認証により通信データの改ざん検知をし，完全性を保証する手法には，メッセージに MAC を

Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

付加する手法が提案されている．[5]では，本来の CAN メッセージに加え，そのメッセージを認証するための MAC 値を別途送信している．そのため通信量が倍以上に増加するといった問題がある．さらに本来の CAN メッセージと MAC 値のメッセージが揃うまで認証が行えないためリアルタイム性が低下するといった問題がある．また業界の動向としては車載ソフトウェアの共通化を実現するためのプラットフォームの仕様の名称，および仕様を策定・公開している団体である AUTOSAR からメッセージに MAC（種類やビット長は未規定）とカウンタ（ビット長は未規定）を付加することで通信データの改ざんを検知して完全性を保証する方式がまとめられた[6]．この手法では，MAC とカウンタのビット長にもよるが，それらを 1 パケットに収めるには既存メッセージ内容を変更する必要があるといった問題がある．

3. 先進運転支援システムの脆弱性評価

本章では，先進運転支援システムに対する攻撃シナリオについて述べ，不正メッセージによるブレーキ制御乗っ取り実験を行った結果を示す．そして先進運転支援システムの脆弱性について調査した結果を報告する．

3.1 先進運転支援システムに対する攻撃シナリオ

従来のなりすまし攻撃の多くはインストルメントパネルへの誤表示，ドアや窓の開閉，エンジン・ブレーキ・ステアリング制御など，対象物に対して直接制御を行っている ECU へ不正なメッセージを送信して行っていた．

一方，我々は先進運転支援システムに着目し，３種類の新たな間接的な攻撃アプローチを提案し，先進運転支援システムを搭載した自動車に対して実車実験を行った結果を報告した[10][12]．各攻撃ポイントを図 2 にまとめた．攻撃ポイント①では，センサーを直接攻撃することで先進運転支援システムに外界の情報を伝えず，システムを無効化させる攻撃を行った．攻撃ポイント②では，システムの作動条件から外す不正メッセージを送信することで自動ブレーキを無効化させる攻撃を行った．攻撃ポイント③では，偽の測距情報を含んだ不正メッセージを送信することで誤発進抑制制御を無効化させる攻撃を行った．

本稿では，ADAS-ECU が発行するメッセージを偽り，自動ブレーキ制御を乗っ取る図 2 の攻撃ポイント④における攻撃について考える．この攻撃ポイントに注目したのは，これまでの実験から ADAS-ECU からブレーキ制御 ECU へ発行するメッセージが 1 種類であった点，ADAS-ECU が発行するメッセージの緊急性が高い点，停止制御自体は安全サイドの制御である点などの観点から，ドライバーによるブレーキ操作との比較や不正メッセージによる乗っ取りの可能性を調査するためである．

CAN メッセージの解析結果より予測した実験に用いた自動車の構成を図 3 に示しておく．通常のドライバーによるブレーキ操作は，ブレーキペダルを踏むことにより発生した油圧が，油圧配管により直接各タイヤのブレーキに送られることで実現されている．一方で自動ブレーキはドライバーによるブレーキ操作と独立して油圧を発生させブレーキをかける必要があるため，ブレーキペダルと各タイヤのブレーキの間に油圧アクチュエーターが接続されている構成となっている．そして，自動ブレーキの際は ADAS-ECU で車両状態（車速，ハンドルやアクセル操作など）に関するメッセージとレーザーレーダーにより取得した距離情報から作動条件の判断が行われ，ブレーキ制御 ECU に対して自動ブレーキ用メッセージの送信が行われる．ブレーキ制御 ECU では，そのメッセージに従い油圧の調整を行うことでブレーキがかかる仕組みである．

次節では，実際に ADAS-ECU からブレーキ制御 ECU に送信される自動ブレーキ用メッセージになりすまして，不正メッセージを送信することでブレーキ制御を乗っ取ることが可能であるか検証した結果について示す．

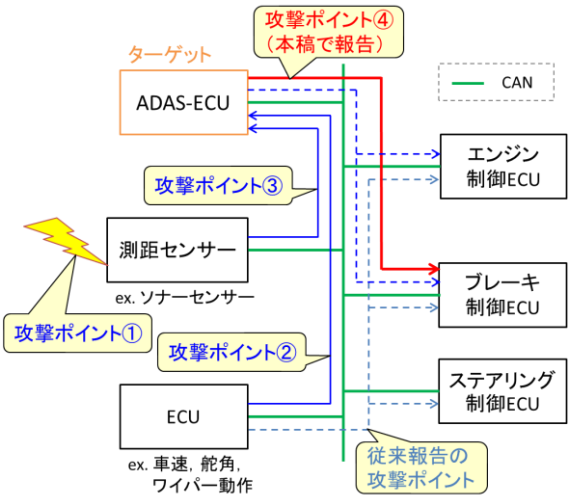

図 2　先進運転支援システムに対する攻撃ポイント

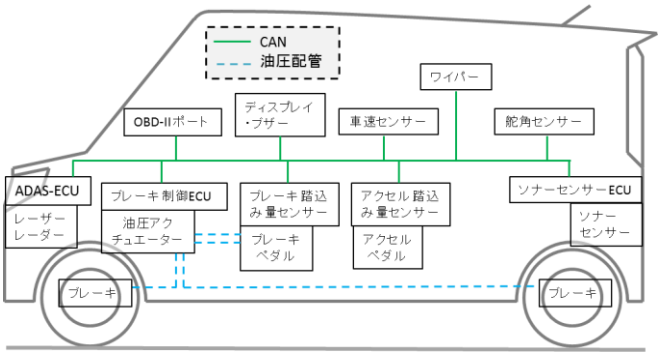

図 3　CAN メッセージの解析結果より予測した実験に用いた自動車の構成

3.2 なりすまし攻撃実験の結果

不正メッセージによるブレーキ制御乗っ取り実験を行った結果を示す．不正メッセージの送信は，OBD-II ポート経

Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

由で CAN バスと接続して行った．

まず正常な動作として，ドライバーによるブレーキ操作時の車速及びブレーキ踏込み量の CAN データのグラフを図 4 に示す．ここで，ブレーキ踏込み量はブレーキを踏んでいない場合が 0 で，踏み込んだ量に応じて値が増加する．グラフより約 14km/h で走行中にブレーキを踏込むことで，徐々に減速していることが確認できる．

次に自動ブレーキ制御乗っ取り時の車速及びブレーキ踏込み量の CAN データのグラフを図 5 に示す．グラフより約 14km/h で走行中にブレーキを踏んでいないにも関わらず一気に減速し，急停車していることが確認できる．これは不正メッセージにより自動ブレーキがかかったことを示している．ちなみに，約 2 秒付近からブレーキ踏込み量が増加しているのは，停車後にドライバーがブレーキ操作を行ったためである．以上の実験結果より，自動ブレーキ用の不正メッセージを送信することによりブレーキ制御の乗っ取りが可能であることが示せた．

自動ブレーキ用の不正メッセージが有効な条件に関しても調査を行った．実験に用いた自動車は，特定の車速の範囲内，且つ前方への走行中にのみ自動ブレーキは作動する仕様であった．しかし，自動ブレーキの作動条件外の車速や自動車がバックしている時も不正メッセージにより急ブレーキをかけることが可能であった．

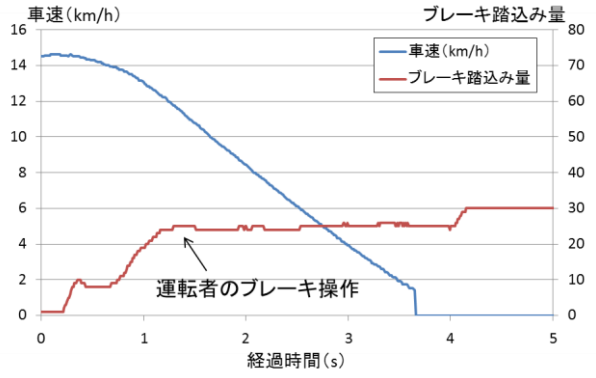

図 4　ドライバーによるブレーキ操作時

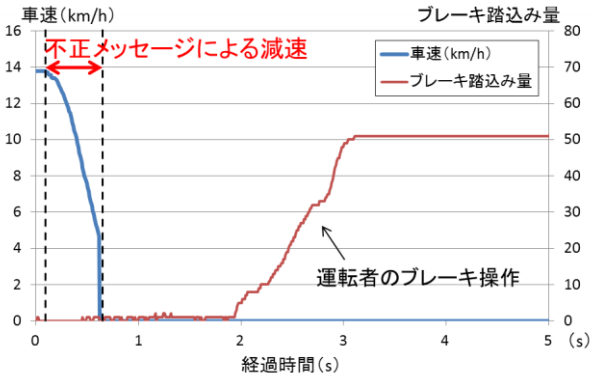

図 5　ブレーキ制御乗っ取り時

3.3 考察

実験結果より自動ブレーキ用メッセージを悪用することで，いつでも不正なブレーキ操作が可能であることがわかった．これは外部から先進運転支援システムに対して攻撃を行うことで，自動車を急停車させて玉突き事故を誘発できる危険性などが考えられる．

我々が調査した限りでは，自動車の「走る，曲がる，止まる」といった基本制御はメッセージの連続性や複数メッセージによる相互判断を行っていると考えられ，制御の乗っ取りは非常に困難であった．実際，アクセル踏込み量に合わせて値が変化するメッセージやデータが複数存在することが確認できており，加速の制御を乗っ取るためにアクセルペダルの踏込み量を感知するセンサーが送信していると考えられるメッセージになりすまし，不正メッセージを送信しても攻撃は成功せずに運転制御を乗っ取ることは出来なかった．そのため，通常の運転制御に対する攻撃を行うには，これらの関連性を理解する必要があり，攻撃を成功させるための難易度は高いと考えられる．

しかし，今回の実験に用いた自動車の自動ブレーキは，ドライバーに危険をいち早く伝える，もしくは衝突を回避するために自動車を安全且つ迅速に停止させることに注力しているためか，インストルメントパネルへの誤表示を行う攻撃と同様に，単一の不正メッセージだけで自動車の停止制御が実現できた．これはセキュリティの観点に立つと，悪意ある攻撃に対する対策が必要不可欠であると考えられる．

次に，この自動ブレーキ制御乗っ取り対策について考察する．まず自動ブレーキ制御が正常に行われた時のメッセージの送信周期を図 6 に示す．通常の走行時には全てのメッセージが周期的に送信されていることが確認できた．最も送信周期が短いもので 10ms 毎にメッセージの送信が行われており，自動ブレーキ用メッセージは 50ms 毎に送信されていた．しかし，自動ブレーキが作動すると，本来の送信周期とは異なるタイミングで自動ブレーキ用メッセージが送信されていることがわかる（図 6 参照）．加えて，他のメッセージの送信周期にも変化が見える．これはセンサー情報より危険を検知して，安全に自動車を停止させるために本来の周期とは異なるタイミングでもメッセージを送信しているものと推測される．このような緊急を要するメッセージが送信周期などを無視して送信されている場合，通信を監視して不正メッセージを検知する対策の適用は困難と考えられる．何故なら，送信周期や送信頻度といった情報は使用できず通信メッセージが正しいかどうかを判断する情報が少ないのと，正規メッセージを誤って撃ち落として事故に繋がる可能性があるのであれば，安全を優先した設計にすることが予想されるためである．

以上より，メッセージ認証により通信データの改ざん検知は最低限必須な対策技術と考えられる．

Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

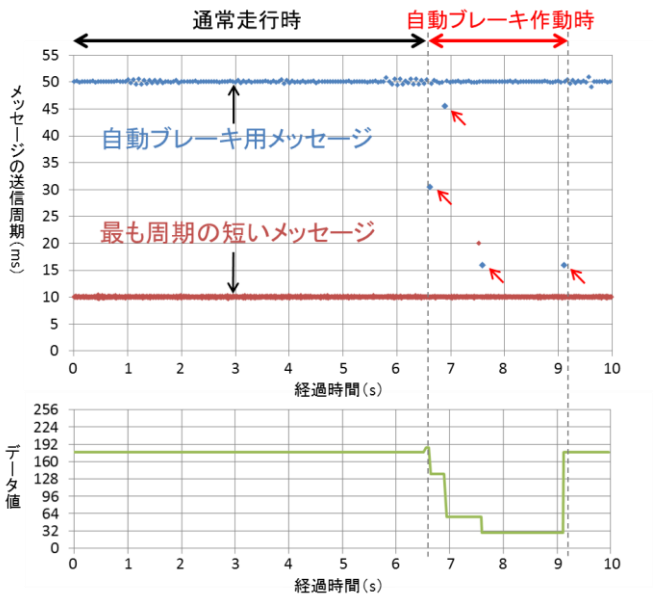

図 6　上：メッセージの送信周期，下：データ値変化

4. 軽量 MAC 認証手法のリプレイ攻撃対策

我々の提案している軽量 MAC 認証手法[10]では，現在までに提案されている MAC を用いる手法と異なり CAN メッセージのペイロード負荷を小さくするために，カウンタ値を別メッセージで配信している．このため，軽量 MAC 認証手法特有のリプレイ攻撃の可能性がある．そこで本章では，軽量 MAC 認証手法のリプレイ攻撃対策を検討した結果について述べる．

4.1 軽量 MAC 認証手法の概要

軽量 MAC 認証手法は CAN メッセージに挿入されているチェックサムを MAC に変更（図 7 参照）して，カウンタに利用する値を別のメッセージとして全ての ECU に配信（図 8 参照）することで，ペイロード負荷を低減した手法である．ペイロード以外の ID や CRC は通常の CAN の規格と全く同一としている．ここで，カウンタ配信用のメッセージを 10ms 周期で 8 バイトとした場合，実験に用いた自動車では約 2.2%通信量が増加する．また，カウンタ値を配信するメッセージもリプレイ攻撃の対象となるため MAC を付加して送信する必要がある．

また，MAC を 1Byte とした場合，不正メッセージを 1/256 の確率で正しいメッセージと認識してしまう可能性がある．しかし車載通信の特徴としてメッセージは一定の周期で繰り返し送信されており，重要な制御に関しては複数のメッセージを受信して多数決で判断することを行っているため，たまたま不正メッセージの MAC が一致して一時的に制御が乗っ取られても，すぐに正規のメッセージにより制御を取り戻すことが可能であると考えられる．

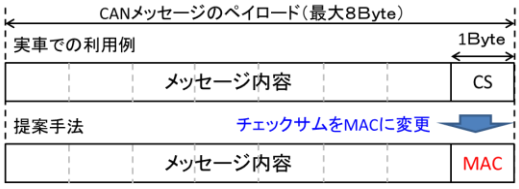

図 7　メッセージ構成

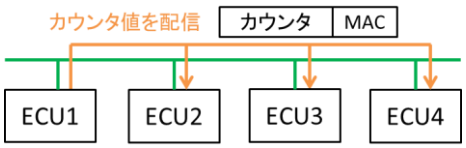

図 8　カウンタ値の配信

また，自動ブレーキ用メッセージでは図 6 に示すようデータ値（メッセージ内容）が段階的に切り替わることがわかっている．そのような場合，連続して不正メッセージを認証してしまう確率は MAC が 1Byte であっても極めて低下する．今回実験に用いた自動車は自動ブレーキがかかった際，メッセージが 4 段階に切り替わっていたので，4 つ全ての不正メッセージを認証してしまう確率は(1/256)^4 となる．そのため，データ値（メッセージ内容）が段階的に変化するメッセージに対しては軽量 MAC 認証を用いた手法で十分有効であると考えられる．

4.2 軽量 MAC 認証手法特有のリプレイ攻撃に対する対策

軽量 MAC 認証手法では，別のメッセージとして配信されるカウンタ値を用いて MAC を算出するため，次のカウンタ値が配信されるまでの間であれば，リプレイ攻撃が可能となる．その理由を以下に示す．

一般的な CAN メッセージの受信と処理は，図 9 に示すような流れで行われる．まず，ECU が CAN バスから受信するメッセージは，ID 毎に設定されたメッセージスロットに保存される．ここで，連続して同じ ID のメッセージを受信した場合，メッセージスロットは上書きされる．そして通常は，割り込み処理によりメッセージを受信する毎に SW 側の変数として保存される．また，連続して同じ ID のメッセージを受信した場合，変数は上書きされ常に最新のデータのみが保持される．そして，タスクが周期的（ここでは 10ms 毎を想定）に起動され，その時点で変数に格納されているデータを用いて処理が行われる．

また，図 10 に示すように軽量 MAC 認証手法では，次のカウンタ値が配信された後は，同じメッセージ内容でも MAC が異なるためリプレイ攻撃は成立しないが，カウンタ値が配信されるまでの間（ここでは 10ms 以内）であれば，あるメッセージを観測して再送することでリプレイ攻撃を行うことは可能である．しかしながら，メッセージの送信処理において，“カウンタ値の配信周期 ≦ 最も周期の短いメッセージの送信周期”の条件を満たす場合，次のカ

Vol.2016-ARC-219 No.3
Vol.2016-SLDM-175 No.3
Vol.2016-EMB-40 No.3
2016/3/24

ウンタ値が配信されるまでの間に，あるメッセージを観測して再送するリプレイ攻撃では，正規のメッセージと同じメッセージを再送することになるため，ECU 内の変数に保持されるデータが正しいデータで更新されるだけであり，攻撃は無効となる．

ここで，カウンタ値の配信周期がメッセージの最小送信周期よりも短い場合，同一のカウンタ値を用いて同じデータに対する MAC 値を算出すると，同じ MAC 値となりリプレイ攻撃が成立してしまう．そのため，カウンタ値の配信周期を最も周期の短いメッセージの送信周期よりも早く，または同じにすることで，軽量 MAC 認証手法特有のリプレイ攻撃に対する対策が可能であると考えられる．

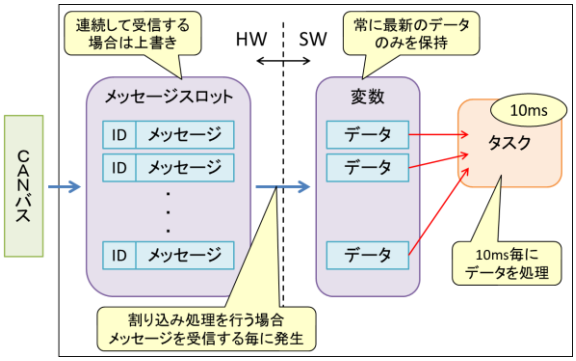

図 9　CAN メッセージの受信と処理のイメージ

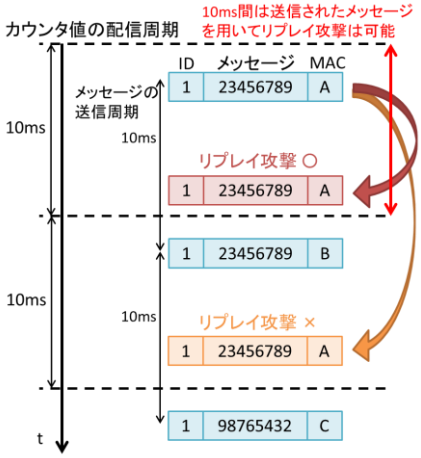

図 10　軽量 MAC 認証手法に対するリプレイ攻撃

5.　まとめと今後の課題

近年急速に普及が進んでいる先進運転支援システムに着目した攻撃手法を検討した．本稿では ADAS-ECU が送信する自動ブレーキ用メッセージを悪用することで，いつでも不正なブレーキ操作が可能であることを実車実験で示した．また，現在の先進運転支援システムでは，安全に直結する重要な制御に関する情報を単一のメッセージで実現していること，ドライバーの制御や誤動作を防止することを優先していること，が不正メッセージによる攻撃を容易にしており，脆弱性に繋がっていることを考察した．

既存の対策手法としては，メッセージの送信周期より異常を検知する手法が提案されているが，先進運転支援システムを搭載する自動車に適用すること困難であると考えられる．その理由として，自動ブレーキのような緊急回避動作時は，通常の送信周期から外れるメッセージが存在することを示した．

我々の提案している軽量 MAC 認証手法は，現在までに提案されている MAC を用いる手法と比較すると CAN メッセージのペイロード負荷は小さいと考えられるが，軽量 MAC 認証手法特有のリプレイ攻撃の可能性が存在した．そこで本稿では，“カウンタ値の配信周期 ≦ 最も周期の短いメッセージの送信周期”とすることで軽量 MAC 認証手法特有のリプレイ攻撃に対策が可能であることを考察した．

今後は，軽量 MAC 認証手法について実装評価を行い，カウンタ値の同期ずれや，リアルタイム性に対する検討を行う予定である．

参考文献

[1] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy 2010.

[2] Charlie Miller, Chris Valasek “Adventures in Automotive Networks and Control Units”, DefCon 21, July, 2013, Las Vegas, NV, USA.

[3] 江崎貴也，伊達友裕，井上博之，“外部ネットワークからの車載 LAN に対する攻撃および防御手法に関する検討”，信学技報，vol.114，no.374，pp.13-18，2014.

[4] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[5] Toyota Infotechnology Center Co., Ltd.,“通信システムにおけるメッセージ認証方法および通信システム” PCT/JP2012/078049, 2013.

[6] AUTOSAR, CAN への MAC 付与，2014. http://www.autosar.org/fileadmin/files/releases/4-2/software-architecture/safety-and-security/standard/AUTOSAR_SWS_SecureOnboardCommunication.pdf

[7] M. Müter, A. Groll, and F. Freiling, “Anomaly Detection for In-Vehicle Networks Using a Sensor-Based Approach,” Journal of Information Assurance and Security, Vol. 6, 2, 2011, pp. 132-140, 2011.

[8] 大塚敏史，石郷岡祐，“既存 ECU を変更不要な車載 LAN 向け侵入検知手法”，情報学会研究報告，2013.

[9] 田邉正人，安齋潤，前田学，氏家良浩，松島秀樹，若林徹，“車載ゲートウェイにおける多層連携 CAN フィルタの提案”，暗号と情報セキュリティシンポジウム 2016.

[10] 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.

[11] Bosh,“CAN Specification Version2.0”, 1991. http://esd.cs.ucr.edu/webres/can20.pdf

[12] 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，“車載測距センサー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.