機械学習による車載ネットワーク攻撃検知システム

Attack Detection System for In-Vehicle Network with Machine Learning

芳賀智之 Tomoyuki Haga
岸川剛 Takeshi Kishikawa
鶴見淳一 Jun-ichi Tsurumi
松島秀樹 Hideki Matsuhima
高橋良太 Ryota Takahashi
佐々木崇光 Takamitsu Sasaki

要　旨

近年，自動車に対するサイバー攻撃として，遠隔から車載ネットワークに侵入し，自動車を不正制御する攻撃事例が報告されており，車載ネットワークとして広く普及するCAN（Controller Area Network）の通信を保護する研究がなされてきた．しかし従来の対策手法は既存のECU（Electronic Control Unit）への改変が必要であり，早期の導入が困難であることが予想される．そこで筆者らはCANを保護するための2つの手法を提案する．1つは，既存の車載システムを変更せずに，CANバスのメッセージを集中監視し，不正メッセージを検知・無効化するCMI-ECU（Centralized Monitoring and Interceptor ECU）である．もう1つが，新種攻撃や攻撃予兆を検知するために，クラウド上での機械学習を用いた異常検知を使った攻撃検知手法である．これら2つの手法を多層にしたシステムを提案し，最後に機械学習を用いて，不正なCANメッセージの異常検知の検証を行い，提案システムの有効性を示す．

Abstract

Controller area network technology (CAN) is widely adopted in vehicles, but security experts have reported that they were able to remotely control a vehicle. Numerous countermeasures have been proposed, but none can be regarded as a generic solution, in part because all the proposed countermeasures require extensive modifications to existing in-vehicle systems. This problem prompted us to develop and propose a security system for connected vehicles. It has two components that protect the CAN. One is the centralized monitoring and interceptor ECU (CMI-ECU) that protects vehicles against malicious CAN messages without the need to modify existing systems. The other component employs an anomaly detection method using machine learning in the cloud to detect new signs of attack so that future attacks can be fended off. Our proposed system protects connected vehicles continuously by linking these two components. Then we verify detection of malicious CAN message by machine learning and show effectiveness of our proposed system.

1. はじめに

近年，自動車内の制御システムは電子化に伴い多数のECU(Electronic Control Unit)と呼ばれる電子制御ユニットと，それらを接続する車載ネットワークによって構成されている．現在，走行や駆動に関わる車載ネットワークの通信規格としてはCAN（Controller Area Network）が広く普及している．CANは車体の軽量化，低コスト化などのメリットがある一方で，セキュリティ上の問題点が指摘され始めている．

まず，2010年に自動車の診断用ポートに攻撃デバイスを装着することでCANを介して自動車を不正制御できることが実証された[1]．この発表をきっかけにCANを介した攻撃実証が相次ぎ，2015年には遠隔から自動車を不正制御できることが実証された[2]．この発表はそれまでと異なり，自動車へ物理的な接触を行うことなく遠隔から不正制御できたことで大きな注目を集め，セキュリティ対策目的としては世界初の140万台のリコールへと発展した．

CANへの攻撃が実証されていく一方で，コネクテッドカーの本格普及も進んでおり，インターネットに接続される自動車の数は，2020年までに2.5億台に達するという報告もある[3]．

このように自動車のインターネットに接続されると，PCと同様に外部ネットワークからのサイバー攻撃の対象となるため，車載ネットワークを保護することは急務となっている．

2. CANの課題

本章では，CANが抱えるセキュリティ課題と，CANを保護する従来技術，その課題について説明する．

2.1 CANが抱えるセキュリティ課題

CANはバス型トポロジをもったネットワークで，ブロードキャストによる通信を行うが，受信側でメッセージの送信元を確認できる機能をもたないため，攻撃者が送信元をなりすまして任意のメッセージを送信できてしまうという課題がある．

2.2 CANを保護する従来技術とその課題

CANにおけるなりすましを防ぐ従来技術は大きく2つある．

［1］MACによるメッセージ認証技術

MACによるメッセージ認証技術は，メッセージ認証コード（Message Authentication Code，以下MAC）を用いた方式である[4]-[6]．これはAUTOSAR[7] (注1) でも標準技術として検討されている．しかし，MACを用いて十分な安全性を確保するためには，認証コードのbit長が少なくとも128 bit必要であると言われているものの，CANメッセージのデータフィールドは最大64 bit足らずであり，1つのCANメッセージのデータフィールド内に認証コードを付与して送信する場合，128 bitの認証コードを64 bit未満に切り捨てる必要があるため，十分な安全性を確保できないという課題がある．128 bitの認証コードを分割して別のCANメッセージとして送信するも考えられるが，送信するメッセージ数が増加し，バス占有率が増えてしまうといった課題もある．また，1台当たり約100個のECUが搭載され，サプライヤも複数あり，全車種・全ECUへの対応は時間を要するという課題がある．

［2］ルールベースによる送信阻止技術

正常なCANメッセージの識別子，データ長，データの上限と下限，送信周期，送信頻度をホワイトリストとして登録して不正検知する手法がある[8], [9]．しかしながら，ルールに基づいた検知手法は，既知攻撃は検知できるが，新種攻撃は検知できないといった課題がある．

3. コネクテッドカー向けサイバー攻撃検知システム

標的型攻撃を始め，IT業界のサイバー攻撃は，高度化しており，従来のルールベースによる検知手法のみでは新種攻撃を検知することが困難となっている．

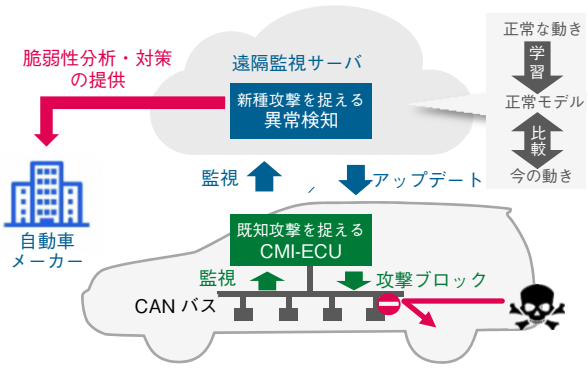
車載向けサイバー攻撃もIT向けの脅威と同様に進化するが予想され，IT業界の対策指針は車載にも適用できると考える．

IT業界では，新種のマルウェアを検知するために，マルウェア，非マルウェアのAPIコールなどの振る舞い情報を特徴量として機械学習を用いた新たな検知技術への取り組みが始まっている．

また，ネットワーク機器のログを収集し，ログをリアルタイムで解析し，異常を検知し，管理者に通知をするSIEM（Security Information and Event Management）が導入されている． SIEMを用いることで，セキュリティインシデントの予兆の発見や，ログ解析による事故発生後の調査などを行うことが可能となる．

3.1 巧妙化するサイバー攻撃への対策方針

攻撃を漏れなくとらえるために，ルールベースによる既知攻撃検知と，機械学習を利用した異常検知技術による新種攻撃検知を多層に配置する車載向けサイバー攻撃検知システムを提案する．提案システムを**第1図**に示す．



第1図　提案システム
Fig. 1　Proposed system

ルールベースによる既知攻撃は，CANバスのメッセージを集中監視し，不正メッセージを検知・無効化するCMI-ECU（Centralized Monitoring and Interceptor ECU）で対策する[10]． また，コネクテッドカーは，常時ネットワーク接続されるため，車両ローカルに配置したCMI-ECUがCANバスに流れるメッセージを監視して，さらに車両情報を遠隔監視サーバにアップロードする．遠隔監視サーバは，アップロードされた車両情報を用いて，機械学習による異常検知により新種攻撃や攻撃の予兆をとらえる．

異常検知の機能を車載デバイスでなく，クラウド側に配置することの利点は3つある．

1つ目は，自動車単体のログに留（とど）まらず，複数の自動車のログに基づいた分析により，多くの車両データの相関から異常検知を行うことや，複数台への大規模攻撃が検知できる点である．

2つ目は，演算リソースが限られており比較的単純なルールベースの検知しか行えない車載デバイスと比べ，遠隔監視サーバは計算リソースが豊富であることから，機械学習を使った高度な異常検知を行うことができる点である．

3つ目は，世界中の自動車の状態を一元化して把握することができるため，攻撃が頻繁に行われる地域や時間帯，車種を特定できる点である．

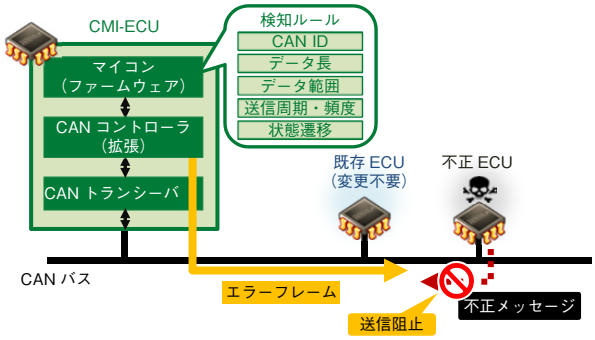
これら3つの利点により，遠隔監視サーバは，車載デバ

（注1）AUTOSAR GbRの登録商標．

イスが検知できない攻撃や攻撃の予兆を検知できる可能性が高い．遠隔監視サーバは，IT向けセキュリティシステムで活用が始まっているSIEM（Security Information Event Management）と似た機能をもつため，Automotive SIEMと呼ぶこともできる．以降で，CMI-ECUと機械学習による異常検知を用いた攻撃検知について説明する．

3.2 CMI-ECUによる攻撃検知

CMI-ECU（Centralized Monitoring Interceptor-ECU）は，CANバスに流れるCANメッセージの監視機能と，ルールベースによる不正検知機能と，CANプロトコルのエラー処理機能を利用した攻撃メッセージの無効化機能を備える．CMI-ECUによる構成を**第2図**に示す．



第2図　CMI-ECU
Fig. 2　CMI ECU

CMI-ECUのルールベースによる不正検知機能は，2種類存在する．

1つ目は，正常な通信メッセージの識別子，データの長さ，データの上限と下限，送信周期，送信頻度をホワイトリストとして設定したルールである．

2つ目は，自動駐車支援，衝突防止，車線逸脱防止などの先進運転支援システムにおける不正な状態遷移を検知するためのルールである．

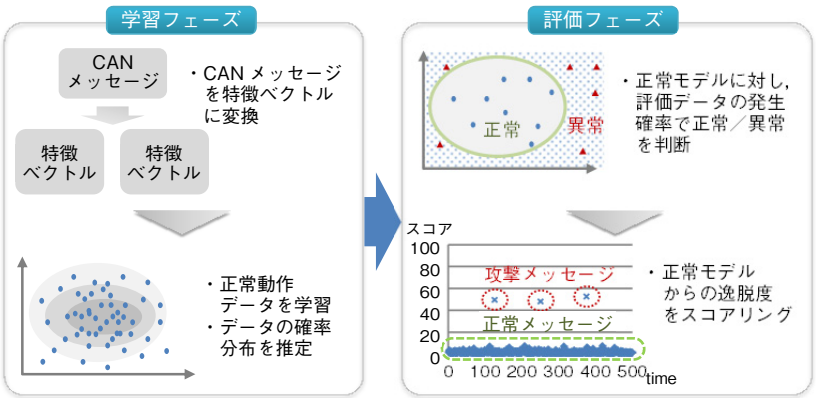
CMI-ECUは，これらの2つのルールに基づいて攻撃メッセージであるかを判断する．CMI-ECUは，不正を検知すると，エラーフレームを送信することで不正メッセージ送信中断を行う．これにより不正メッセージを無効化することで，車両の不正制御を防止する．

また，CMI-ECUは，CANメッセージを記録し，常時もしくは定期的に遠隔監視サーバへアップロードする．しかし多くの自動車がCANメッセージを常時アップロードすることは，遠隔監視サーバの回線輻輳（ふくそう）や記憶領域不足などの原因になる．この課題を解決するためには，遠隔監視サーバに送信するCAN通信メッセージを削減する必要がある．送信するCAN通信メッセージを削減する方法として，一定時間ごとサンプリングしたCANメッセージを遠隔監視サーバに送信する方法や，走る・曲がる・止まるといった制御に関わるメッセージに種類を限定して送信する方法などが挙げられる．

3.3 機械学習を用いた異常検知

機械学習を用いた異常検知手法として，大きく教師あり学習と教師なし学習が存在する．教師あり学習の異常検知では，個々の学習データに対して，正常と異常のラベルを付与して学習することで，評価対象のデータが，正常もしくは異常のどちらのラベルに分類されるかを判別する手法である．一方，教師なし学習の異常検知は，正常なデータのみを学習データとして学習し，正常以外のデータを異常と判別する検知手法である．本システムにおいては，既知攻撃だけでなく，CMI-ECUで検知することが困難な新種攻撃を検知するため，教師なし学習の異常検知を採用した．本システムでは，クラウド上の遠隔監視サーバに異常検知処理を実装し，異常メッセージを検知することで新種攻撃をとらえる．

教師なし学習の異常検知アルゴリズムは，**第3図**に示



第3図　教師なし機械学習による異常検知
Fig. 3　Anomaly detection with unsupervised machine learning

すように，学習フェーズと評価フェーズからなる．学習フェーズでは，学習データとなる正常な動作を示すCANメッセージを特徴ベクトルに変換し，正常な通信メッセージの振る舞いを示す正常モデルを生成する．そして，評価フェーズでは，学習フェーズで生成した正常モデルに対して逸脱した通信メッセージを異常メッセージとして検知する．評価フェーズでは，正常モデルからの逸脱度をスコアとして算出し，スコアの高いメッセージを異常として検知する．

本システムを利用する分析官は，スコアが高いメッセージから優先的に解析を行うことで，新種攻撃を分析し，新種攻撃に対応した検知ルールを効率的に作成することができる．作成した検知ルールをCMI-ECUに配布し，CMI-ECUの検知ルールをアップデートすることで，以降同様の攻撃に対しては，自動車内部に配置したCMI-ECUで検知して，送信阻止を行うことが可能となり，検知性能が向上する．

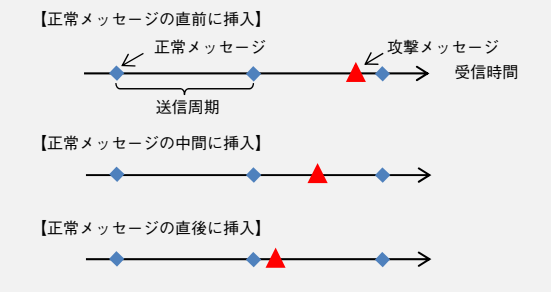
4. 機械学習を用いた異常検知手法の検証

本章では，前章で考案した教師なし異常検知アルゴリズムを用いた不正検知手法の有効性検証結果について説明する．教師なし異常検知アルゴリズムとして，外れ値検知アルゴリズムが知られている．その1つとして点の密度をベースに，ある点の異常度合いをスコアとして算出するLOF（Local Outlier Factor）[11]で検証した．LOFでは，密度の低い点ほど高いスコアとなり，異常度合いが分かる．また，検知対象の攻撃として，自動車の操舵（そうだ）角の改ざん攻撃を想定した．

まず，学習フェーズで実車から収集したCANメッセージのログのうち，操舵角を示す正常な通信メッセージの送信周期とデータ変化量の2つを用い正常モデルを作成した．学習に利用したCANメッセージのログは，約80秒間通常走行したときのものを用いた．

次に，実車から取得したCANメッセージのログに，操舵角の改ざん攻撃メッセージを静的に注入した評価データを作成した．攻撃メッセージは，従来のルールベースの検知手法では検知できないメッセージとすることを意図して作成した．つまり，操舵角を示す正常な通信メッセージを装うため，識別子，データの長さなど，メッセージのフォーマットはすべて正常値とした．ただし，操舵角を示すデータ値を上限値に設定した．これは攻撃者が自動車に急旋回させようとする意図を再現している．

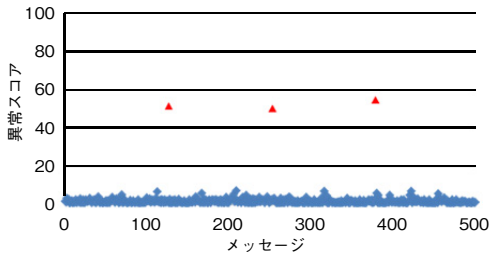
次に，作成した攻撃メッセージを実車のCANメッセージのログに挿入し検証データを作成した．挿入する攻撃メッセージは3つとし，それぞれ挿入タイミングを変えた．挿入タイミングは，**第4図**に示すように，正常メッセージの直前，正常メッセージの中間，正常メッセージの直後の3つである．



第4図　挿入パターン
Fig. 4　Patterns of insertion

最後に，評価フェーズにおいて，正常モデルに基づき，検証データのなかの攻撃メッセージを検知できるか検証した．検証は，検証データ（CANメッセージのログ）に含まれる通信メッセージを順に読み込み，通信メッセージ単位で異常スコアを算出することで行う．

検証結果を**第5図**に示す．図の縦軸は受信したメッセージの異常スコアを示す．図の横軸は読み込んだメッセージの順番を示す．図の四角（◆）は正常メッセージを示し，三角（▲）は攻撃メッセージを示す．



第5図　評価データのスコア
Fig. 5　Score with evaluation data

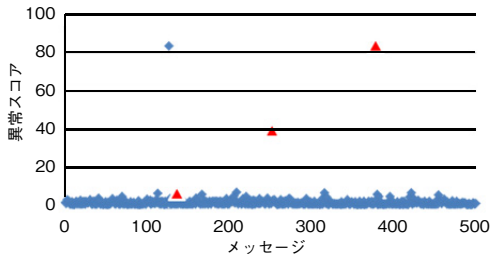
第5図が示すように，3つの攻撃メッセージの異常スコアが，正常メッセージと比較して高い値を示し，攻撃メッセージを検知できたことが分かる．

異常スコアを解析した結果，データ変化量の異常スコア値が特に大きく算出されていることが判明した．LOFを使った外れ値検知手法が，データ変化量の振る舞いの異常をとらえ，攻撃メッセージを検知していることが分かる．

そこで，データ変化量の少ない攻撃メッセージを検知できるか追加の検証を行った．追加の検証データは，攻撃メッセージのデータ値を，直前の正常な通信メッセー

ジのデータ値と同じ値に設定した．それ以外は，既に作成した検証データと同じとした．これは攻撃者が自動車を徐々に旋回させようとする意図を再現したもので，高度な攻撃と言える．

追加の検証結果を**第6図**に示す．図の縦軸と横軸は**第5図**と同じである．



第6図　追加評価データのスコア
Fig. 6　Score with additional evaluation data

第6図が示すように，3つの攻撃メッセージのなかで，2つの攻撃メッセージの異常スコアが高くなり検知できたが，正常メッセージの直前に挿入した攻撃メッセージは，周期およびデータ値が正常値に近いため正常と判定され，攻撃メッセージ直後の正常メッセージのスコアが高く算出される結果となった．

追加検証で対象とした3つの攻撃メッセージは，データ変化量を直前の正常メッセージと同じ値に設定したため，正常な通信メッセージとの振る舞いの違いが，送信周期に限定される．そのため，正常な通信メッセージの直前に挿入した攻撃メッセージは，送信周期の観点で異常がないと判定されてしまい，攻撃メッセージ直後の正常メッセージのスコアが高く算出される結果となった．

しかしながら，異常が起きていることは確認できる．そのため，スコアが高いメッセージ付近を精査することで攻撃検知につなげることができると考える．

5. まとめ

本稿では，CANバスを集中監視しルールベースによる不正検知・無効化するCMI-ECUと，遠隔監視サーバによる機械学習を用いた異常検知を多層化した攻撃検知システムを提案した．異常検知アルゴリズムはLOFを利用し，操舵角の偽装攻撃検知の実験を通して，本システムの有効性を検証した．

データ値を最大値に設定したメッセージを注入する攻撃は検知することができた．一方，正常なデータ値に設定したなりすましメッセージを正常メッセージの直前に注入する攻撃は，注入した攻撃メッセージ直後の正常メッセージのスコアが高く算出され，攻撃メッセージの特定はできなかった．しかしながら，異常が起きていることは検知できるため，高スコア付近のメッセージを精査することで攻撃検知につなげることができると考える．

また，本検証では攻撃者の想定が少なく，さらに定性的な評価しか行われていない．将来的には定量的な評価を行うために，検知率などの指標を用いて評価する必要がある．また異常検知アルゴリズムの選定も必要である．例えば，LOF以外の，One-Class SVM（Support Vector Machine）[12]やIsolation Forest[13]などの複数の異常検知アルゴリズムを併用して異常をとらえることが考えられる．

また，現時点においても，攻撃を検知することができないものの，攻撃前後のメッセージの異常スコアが高く算出されるため，攻撃の検知には至らずとも，攻撃が発生していることは把握することができる．そのため，ドライバーに警告を出したり，自動運転機能など攻撃対象機能をオフにしたりすることなど，被害を抑止する手法について検討することができると考える．

また，自動車のセキュリティ情報を共有する組織Auto-ISAC（Information Sharing and Analysis Center）が設立され，自動車に対するサイバー脅威や脆弱（ぜいじゃく）性について情報共有や分析や対策検討をする組織も立ち上がっている．本システムにより，Auto-ISACのような組織や自動車メーカーに対して，攻撃分析結果や攻撃への対策案の提供が可能であると考える．

本システムの技術を用いて，安心・安全なコネクテッドカーや自動運転社会の実現に貢献していく．

参考文献

[1] K. Koscher et al, “Experimental security analysis of a modern automobile,” IEEE Symposium on Security and Privacy, Oakland, May 2010.
[2] C. Miller et al., “Remote Exploitation of an Unaltered Passenger Vehicle,” DEF CON, Las Vegas, July 2015.
[3] Gartner, Inc., “Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities,” http://www.gartner.com/newsroom/id/2970017, 参照 Apr. 19. 2017.
[4] B. Glas et al., “Signal-based Automotive Communication Security and Its Interplay with Safety Requirements,” Embedded Security in Cars, Berlin, Nov. 2012.
[5] O. Hartkopp et al., “MaCAN – Message Authenticated CAN,” Embedded Security in Cars, Berlin, Nov. 2012.
[6] D. K. Nilsson et al., “Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes,” Vehicular Technology Conference, Calgary, Sep. 2008.
[7] AUTOSAR, http://www.autosar.org/, 参照 Apr. 19. 2017.
[8] T. Hoppe et al., “Security threats to automotive CAN networks –

Practical examples and selected short-term countermeasures," Proceedings of the 27th international conference on Computer Safety, Reliability, and Security, pp. 235-248, Sep. 2008.

[9] S. Otsuka et al., "Intrusion Detection for In-vehicle Networks without Modifying Legacy ECUs," IPSJ SIG Technical Report , vol. 112, no. 481, pp.31-35, 2013.

[10] Y. Ujiie et al., "A Method for Disabling Malicious CAN Messages by Using a Centralized Monitoring and Interceptor ECU," Embedded Security in Cars, Cologne, Nov. 2015.

[11] Markus M. Breunig et al., "LOF: Identifying Density-Based Local Outliers," http://www.dbs.ifi.lmu.de/Publikationen/Papers/LOF. pdf, 参照 Apr. 19. 2017.

[12] V. Vapnik et al., "Pattern recognition using generalized portrait method," Automation and Remote Control, vol. 24, pp.774-780, 1963.

[13] Liu F.T. et al., "Isocation based anomaly detection," ACM Transactions on Knowledge Discovery from Data, vol. 6, no. 1, pp. 1-39, 2012.

執筆者紹介

芳賀　智之　Tomoyuki Haga
ビジネスイノベーション本部
AIソリューションセンター
AI Solution Center,
Innovation　Business Innovation Div.

岸川　剛　Takeshi Kishikawa
ビジネスイノベーション本部
AIソリューションセンター
AI Solution Center,
Innovation　Business Innovation Div.

鶴見　淳一　Jun-ichi Tsurumi
ビジネスイノベーション本部
AIソリューションセンター
AI Solution Center,
Innovation　Business Innovation Div.

松島　秀樹　Hideki Matsuhima
ビジネスイノベーション本部
AIソリューションセンター
AI Solution Center,
Innovation　Business Innovation Div.

高橋　良太　Ryota Takahashi
製品セキュリティセンター
Product Security Center

佐々木　崇光　Takamitsu Sasaki
製品セキュリティセンター
Product Security Center