CANにおけるエラーフレーム監視機構の提案

倉地 亮† 高田 広章† 上田 浩史‡ 堀端 啓史‡

†名古屋大学大学院情報科学研究科
464-8601 名古屋市千種区不老町 NIC 508
kurachi@nces.is.nagoya-u.ac.jp, hiro@ertl.jp

‡株式会社オートネットワーク技術研究所/住友電気工業株式会社

510-8503 三重県四日市市西末広町 1 番 14 号
ueda-hiroshi@sei.co.jp, horihata@sei.co.jp

あらまし Controller Area Network (CAN) が車載制御ネットワークに広く使用されており，近年，CAN に対する様々なセキュリティ攻撃方法が提案されている．このため，自動車メーカでは，CAN に対するなりすましメッセージ，ソフトウェアの改ざん，DoS 攻撃などの様々なセキュリティ攻撃への対策手段が必要とされている．本研究では，我々が提案する集中型セキュリティ監視システム (CaCAN: Centralized Authentication CAN) をベースとし，エラーフレームを監視することにより，セキュリティ攻撃や異常の有無を検出することを目的としている．

Proposal of the error frame monitoring system with improved Controller Area Network (CAN) controller

Ryo Kurachi† Hiroaki Takada† Hiroshi Ueda‡ Satoshi Horihata‡

†Information Science, Nagoya University.
NIC 508, Furo-cho, Chikusa-ku, Nagoya, Aichi 464-8601 JAPAN
kurachi@nces.is.nagoya-u.ac.jp, hiro@ertl.jp

‡AutoNetworks Technologies, Ltd./Sumitomo Electric Industries, Ltd.
1-14 Nishi-Suehiro-cho, Yokkaichi, Mie 510-8503, JAPAN
ueda-hiroshi@sei.co.jp, horihata@sei.co.jp

Abstract Recently, security attacks in vehicles have been increasing and have been reported in several papers. In particular, Controller Area Network (CAN) suffers from some common disadvantages such as limited baud rate and payloads. Therefore, OEMs requires countermeasures against several security attacks such as spoofing messages, malicious software and Derial of Services (DoS). Therefore, we proposed the CaCAN (Centralized Authentication Systems in CAN) where the monitor node employs the improved CAN controller against security attacks. In this paper, we propose the error frame monitoring features for CAN network with improved CAN controller.

1　はじめに

特に，Controller Area Network (CAN) [1] は，車載制御ネットワークの中で最も広く使われているプロトコルであり，現在販売されている多くの車両に搭載されている．近年，CAN はセキュリティに対しては脆弱であることが多数の研究で指摘されており，対策技術が必要とされている．しかしながら，CAN では最大転送レートが 1Mbps，最大ペイロード長が 8Bytes に制約されており，既存する情報セキュリティ技術をそのまま適用することが難しいことが課題である．

また，現在販売されている車両の多くではセキュリティ対策が講じられておらず，CAN への最も深刻な攻撃はなりすましメッセージを注入することであり，メーターの表示やブレーキの無効化といった異常な制御を引き起こすことが可能であることが既存研究により示されている [2, 3, 4].

1.1　関連研究

我々の先行研究及び複数の既存研究では，不正な CAN メッセージをエラーフレームで上書きすることにより排除する手法が提案されている．

松本らは，正規ノードが CAN のエラーフレームを用いて不正メッセージを排除する手法を提案した．この手法では，すべての正規ノードが改造された CAN コントローラを用いて，攻撃ノードから送信される CAN メッセージの識別子（CAN-ID）を用いて，CAN を検査する手法を提案している [5].

芳賀らは，静的に決定される通信仕様に着目し，使用されない CAN メッセージ (ID や DLC など) を検出する場合に不正メッセージと判断し，エラーフレームを用いて排除する手法を提案した [6].

我々の先行研究では，松本らの既存手法を改良し，CAN メッセージのペイロードに付与される Message Authentication Codes(MAC) を検査し，監視ノードが MAC の異常を検出する場合には，即時エラーフレームで上書きすることで，不正なメッセージの伝播を阻止する手法を提案した [7].

また，欧州を中心とする自動車業界でもセキュリティ対策技術の検討が進められており，AUTomotive Open System ARchitecture (AUTOSAR) では Secure onborad communication (SecOC) の仕様として，CAN メッセージのペイロードに MAC を付与することを規定している [8].

1.2　先行研究

我々が提案する集中型セキュリティ監視システムでは，不正なメッセージを CAN メッセージのペイロードに付与されたメッセージ認証コード (MAC) が正しいかどうかを監視ノードのみが判断し，もし MAC が誤っている場合には，そのフレームを監視ノードがエラーフレームで打ち落とす方式である (図 1)．しかしながら，すべての CAN メッセージに MAC を付与することは，既存するすべての ECU のプログラムを変更しなければならず，必ずしも容易に実現できるものではない．このため，我々は真に重要な一部のメッセージにおいては MAC を付与することを想定している一方，MAC が付与されない CAN メッセージに対しては，その振る舞い (送信タイミング) を監視することで，不正な CAN メッセージを検出する手法を提案している [9].

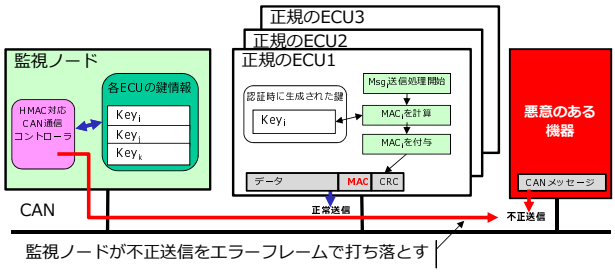

図 1: 集中型セキュリティ監視システム

1.3 本研究の位置付け

前述するセキュリティ対策を適用した車載制御システムにおいては，CAN ネットワーク上に不正な CAN メッセージが流れるとエラーフレームが送出される．これは，従来，伝送路上のノイズや断線，ノードの異常動作などの故障時だけでなく，セキュリティ上の異常検出時にもエラーフレームが CAN バス上に送信される可能性があることを示唆している．

このような理由から，今後は，エラーフレームが CAN バス上に送出される要因やタイミングを収集し，どのような異常が発生したかを分析することは非常に重要であると考えられる．

2 CAN におけるエラーフレーム

CAN では，どういう要因でエラーフレームを送信したかをエラーフレームの受信ノードが知ることはできない．このため，同一 CAN バス上にセキュリティ対策処理が分散されていると，故障要因とセキュリティ要因の異常検出要因の区別がつかないという課題がある．以降では，その詳細について述べる．

2.1 エラーフレームの発生要因

CAN では，プロトコル仕様上以下の 5 つのエラーが送出されることが規定されている．

1. ビットエラー: 送信ノードあるいは受信ノードにて，送出しているバスの信号レベルと自身の送出したいバスの信号レベルが不一致 (尚，アービトレーションフィールドと ACK フィールドは対象外)
2. スタッフエラー: 送信ノードあるいは受信ノードにて，ビットスタッフが行われているはずのフィールドにて，同一レベルを 6 ビット連続して検出するエラー．
3. フォームエラー: 送信ノードあるいは受信ノードにて，フレームフォーマット上の固定ビットフィールドにおいて定義されていない信号レベルを検出したことによるエラー．
4. CRC エラー: 受信ノードが受信した CAN フレームの CRC を検査した結果，CRC に異常があると検出する場合に検出されるエラー．
5. ACK エラー: 送信ノードが ACK スロットにて，レセシブレベルを検出したことによるエラー．

ある CAN フレームがバス上へ送出されている際，送信あるいは受信ノードにおいて，これらの異常が検出されると，送信するノード及び他の受信ノードに対してその CAN フレームを破棄するようエラーフレームが送出される．

また，関連研究 (1.1 節) で提案されるエラーについては，プロトコル仕様として追加し，既存する CAN コントローラのハードウェアを改造することで，以下のエラーの検出が可能になる．

1. Unknown メッセージエラー [5, 6]: システム構成上，使用されるはずのない CAN メッセージがバスに送出されたことを表す．また，文献 [5] にて定義される正規ノード以外のノードが送出する CAN メッセージについても同様とする．
2. MAC エラー [7]: 受信ノードにて計算した Message Authentication Code(MAC) と受信した CAN フレームに付与されている MAC の不一致によるエラー．
3. DLC エラー [6]: 静的に与えられるデータフォーマットにおいて，運用上使用されないはずのデータ長が指定される場合に検出されるエラー．

2.2 エラーフレームの発生要因分析の課題

CAN の仕様上，エラーフレームを受信するノードでは，以下の理由によりその発生要因を知ることはできない．(1) エラーフレームの送信ノードは判別できない．つまり，エラーフレームを送信しているノードが正規ノードか，それとも攻撃者が物理的に設置した不正なノードかどうかを判断することはできない．また，(2) エラーフレームを受信するノードではそのエラー

フレームの発生要因は判断できない．例えば，エラーフレームの検出時にエラーが発生したビットを推定した上で，その発生要因を一意に特定することは難しい．このため，エラーフレームの受信ノードでは正確なエラーフレームの発生要因を知ることができない．

これらの理由から，本論で提案するエラーフレーム監視を行う場合には，エラーフレームを監視するノードがセキュリティ監視を行う方が効率が良いといえる．

3 エラーフレーム監視機構の提案

3.1 セキュリティゴール

本論では，提案するエラーフレーム監視機構により，エラーフレームの発生要因を分析することでセキュリティ上の侵害あるいは異常を検出し，速やかにシステムの安全状態へと遷移させることを目的とする．尚，故障とセキュリティ上の攻撃を判断することは難しいため，本論文では区別しないものとして扱う．

3.2 検出したい異常

エラーフレーム監視機構を用いて，以下のシステム異常を検出することを目的とする．

- ある特定の CAN メッセージに対して発生するエラーフレーム: 攻撃者が不正ノードを設置し，ある正規 ECU のなりすましを実施する場合，ある特定の CAN メッセージに対してエラーフレームが発生することが予想される．このため，攻撃目標となっている CAN メッセージを特定し，その攻撃対象を排除することで，なりすましメッセージを排除することを目的とする．
- ある特定の CAN メッセージへの攻撃からどの ECU に異常が発生しているかを特定する．

3.3 提案するフレームワーク

我々の提案する手法では，エラーフレーム発生時の情報を収集できるよう改造された CAN コントローラを使用する．エラーフレーム発生時に収集される情報は以下のとおりとする．

1. CAN-ID: エラーフレームが発生した CAN フレームの CAN-ID(識別子) を記憶し通知する．
2. エラー発生フィールド: エラーフレームが発生した CAN フレームのエラー発生フィールドを記憶し通知する．

図 2 に示すように，これらの情報を用いて，エラーが発生したメッセージを特定し攻撃者の攻撃目標を特定するものである．

3.4 攻撃対象メッセージの特定

エラーフレーム発生時の CAN-ID を識別により，どの CAN メッセージが攻撃者に狙われているかを区別することを目的とする．このため，エラーフレームが発生した CAN フレームの CAN-ID 部分を記憶しておくよう CAN コントローラを改良した上で，以下の図 2 の方法により攻撃対象メッセージの特定を実地する．

この図に示すとおり，(1) 監視ノードは，まずエラーフレームが発生するノードの情報を収集することにより，攻撃対象を特定する．次に，(2) エラーフレームの累積状況から故障/攻撃対象ノードの異常を判定し，それらのノードの送出される異常を切り離す必要がある．

4 セキュリティ分析

4.1 提案手法では対策できれない脅威や攻撃

本対策手法に対するセキュリティ攻撃としては，以下の攻撃が想定される．

1. エラーフレーム送信: エラーフレームを故意に送信することにより，ある CAN メッ

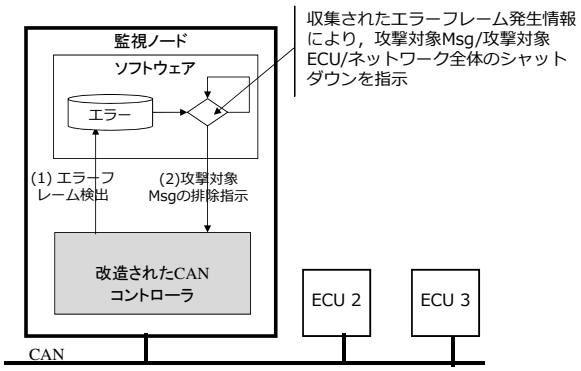

図 2: 提案するフレームワーク

セージの通信を途絶することを可能にする．しかしながら，我々のシステムでは，異常を検出した CAN メッセージは以降すべての正規/なりすましメッセージも排除するよう設計されているため，これにより機能が縮退するなどの影響はあるものの，より被害が甚大ななりすましメッセージの送信を防止することは可能である．

2. 物理的に監視ノードを CAN バスから途絶と中間者攻撃：車載制御ネットワークの大半は物理的に保護されてないため，物理的なバスの改造により，容易に途絶することは可能である．このため，攻撃者が物理的に不正なノードを設置することにより，監視ノードを監視対象バスから隔離する場合には，中間者攻撃が実現可能になる．この場合，監視ノードが監視対象バスにて観測するべきエラーフレームが中間者ノードにより監視できない．

5 実装と評価

提案するエラーフレーム監視機構を検証するために，改造された CAN コントローラが必要となる．このため，我々はアルテラ社製の DE2-115 開発ボードを用いて実装した．このボード上の FPGA に，CAN コントローラ，NiosII ソフトコア，DRAM などにより構成し，NiosII ソフトコア上のソフトウェアとしては TOPPERS ATK2 を用いて実装した．本提案手法を実現するために，まず，エラー検出を実現する改良された CAN コントローラを実装した．この CAN コントローラでは，前述の提案手法に記載されるように，エラーフレームの発生状況を分析できるようエラー情報を付与する構成とした．

5.1 評価 1: MAC エラーに関する分析

MAC エラーが発生したときに，その該当する CAN メッセージが正しく判定できるかどうかを検証した．その結果，すべての MAC エラーが発生するときには，該当する CAN メッセージが正しい CAN-ID を識別した．

6 まとめ

近年，車載制御ネットワークを通じた攻撃事例が報告されており，これまでに幾つかのエラーフレームを用いた対策手法が提案されている．本論では，集中型セキュリティ監視システムにおいて，エラーフレームを用いた異常検出手法を提案した．今回，我々が提案する MAC エラーを対象として，実機上で正しくエラー情報を収集できること及び，従来よりも正確な異常判定が可能であることを示した．また，今後の課題として，エラーフレームを利用したセキュリティ上の異常と故障の判別手法の検討が挙げられる．

参考文献

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

[2] K. Koscher, et al.,“ Experimental Security Analysis of a Modern Automobile, ”IEEE Symposium on Security and Privacy 2010, pp.447-462, 2010.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno Comprehensive Experimental

Analyses of Automotive Attack Surfaces", USENIX conference on Security, 2011.

[4] Charlie Miller, Chris Valasek Adventures in Automotive Networks and Control Units", DEFCON 21, 2013.

[5] Matsumoto, T., Hata, M., Tanabe, M., Yoshioka, K. et al.," A Method of Preventing Unauthorized Data Transmission in Controller Area Network, "Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, 2012.

[6] 芳賀 智之, 氏家 良浩, 岸川 剛, 松島 秀樹, 田邉 正人, 北村 嘉彦, 安齋 潤, 車載ネットワークを保護するセキュリティECU の提案：導入インパクトを抑えた CAN 保護手法のコンセプトとその評価, SCIS2015, Jan 2015.

[7] Kurachi, R., Matsubara, Y., Takada, H., Adachi, N., Miyashita, Y., and Horihata, S., "CaCAN - Centralized Authentication System in CAN", Proceedings of the escar 2014 Europe Conference, Hamburg, Germany, Nov 2014.

[8] Autosar version 4.2.1, Requirements on Module Secure Onboard Communication, AUTOSAR_SRS_SecureOnboardCommunication.pdf `http://www.autosar.org/`, Aug, 2015.

[9] 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. Jan 2015.