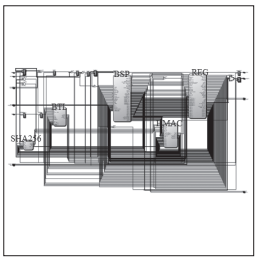

車載ネットワークのセキュリティ監視システム

Security Authentication System for In-Vehicle Network

上田　浩史* Hiroshi Ueda
倉地　亮* Ryo Kurachi
高田　広章 Hiroaki Takada
水谷　友洋 Tomohiro Mizutani
井上　雅之 Masayuki Inoue
堀端　啓史 Satoshi Horihata

車載制御ネットワークに広く利用されているController Area Network (CAN) に対して、なりすましメッセージを注入することで、車の制御を乗っ取る攻撃事例が報告されている。このため、リアルタイム性やコスト制約の厳しい車載制御ネットワーク特有の要件を満たしたセキュリティ対策手法が望まれている。本稿では、改良したCANコントローラを用いたCANのセキュリティ監視システムについて提案する。さらに、試作基板を用いて評価を行った結果についても報告する。

One of the main concerns for the security of in-vehicle data is spoofing messages on the in-vehicle network. Controller Area Network (CAN) is the most extensively embedded network protocol in vehicles. In the last decade, security attacks in vehicles have been increasing and have been reported in several papers. Therefore, security measures are expected that meet the requirements of real time and cost constraint for in-vehicle control network. In this paper, we propose centralized authentication system in CAN with improved CAN controller. Our experimental results demonstrate that our proposed method is effective on real in-vehicle network environments.

キーワード：車載セキュリティ、車載制御ネットワーク、Controller Area Network (CAN)

1. 緒　　言

現在の自動車には、1台あたりおよそ70個以上のElectronic Control Unit (ECU) と呼ばれる電子制御ユニットが搭載されており[1]、Controller Area Network (CAN)[2]、Local Interconnect Network (LIN)[3]、FlexRay™ [4] などに接続され、その制御を実現している。特にCAN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車両の多くに搭載されている。ところが、CANはセキュリティに対しては脆弱であることが指摘されている。CANへの攻撃事例として、なりすましメッセージを注入することで、メーターの表示改ざんや、ブレーキの無効化といった不正制御が可能なことが実証されている[5]。一方で、CANは最大転送速度が1Mbpsであり、1メッセージのペイロードも最大8バイトであることから、これまで民生技術で培われてきた対策手法をそのまま適用することが難しいという制約も存在する。

そこで本稿では、改良したCANコントローラ※1を用いたCANの集中型セキュリティ監視システムを提案する。FPGA (Field-Programmable Gate Array) を用いた試作基板でタイミング検証を行い、本提案方式が実現可能であることを実証した。

2. CANにおけるセキュリティリスク

2－1　CANの特徴

車載制御システムで広く使用されるCANは、ISO11898およびISO11519で標準化された通信プロトコルであり、OSI 参照モデルの第1層と第2層を中心に規定されており、その特徴は以下のとおり挙げられる。

(a) バストポロジ

1つの通信線に複数のECUが接続されるバストポロジで広く使用されている。

(b) マルチマスタ

各ノードは、送信したいメッセージがあるとすぐにCANバス上へとメッセージを送信することができる。このため、容易にCANメッセージやノードを追加することができる。

(c) 送信権の調停

複数のノードが同時にCANバス上へメッセージを送信すると、CAN-IDを用いた送信権の調停が実施される。この結果、最も優先度の高いメッセージを持つCANメッセージが優先的に送信されるため、優先度の低いメッセージはより高い優先度のメッセージの送出が完了するまで遅延させられる。

2－2　CANのセキュリティリスク

これまでの攻撃事例[5]より、CANにおける、なりすまし攻撃には以下の2つのユースケースが想定される。

ユースケース1：ECUソフトウェアの不正書き換え
図1は正規ECUが悪意あるプログラムに書き換えられ、なりすましメッセージを送信する例である。

ユースケース2：不正機器の接続
図2はCANバス上につながれた不正機器がなりすましメッセージを送信する例である。

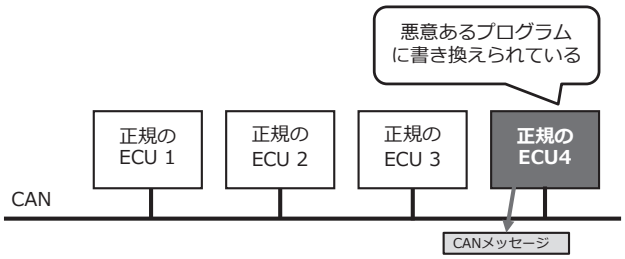

図1　正規ECUの悪意あるプログラムへの書き換え

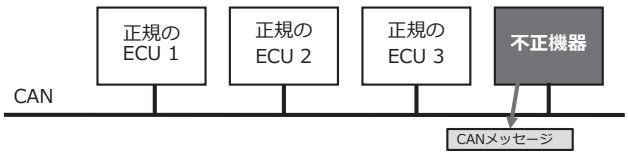

図2　不正機器の接続

3.　CANのセキュリティ対策手法

3−1　従来研究

近年、車載制御システムに対する多くの攻撃事例が報告される一方、これらの攻撃に対抗するための対策手法についても数多く検討されている[6]〜[10]。しかしながら、これらの手法では、ネットワーク上に配置されるすべてのノードに対策を実施する必要があることが課題である。

3−2　提案手法：セキュリティ監視システム

本稿で提案するセキュリティ監視システムの概要を**図3**に示す。前述のようにCANプロトコルは認証が存在しないため、なりすまし攻撃に対して脆弱である。本提案手法ではなりすましに対して一般的に効果があるといわれているメッセージ認証コード（MAC：Message Authentication Code）※2を用いることとした。

本提案手法では監視ノードが各ECUを認証し、CANメッセージに付与されるメッセージ認証コードを検証することでなりすまし攻撃に対抗することを目的としている。監視ノードには特別なCANコントローラを実装する必要がある。この特別なCANコントローラがなりすましメッセージをリアルタイムにエラーフレームを用いて上書きする。本提案手法の優れている点はCANバス上に存在する監視ノードのみハードウェアの改造を行えばよいという点である。それゆえ、他のECUはノード認証や鍵交換を行うためのソフトウェアの改修のみで実現できる。

送信ノード（正規のECU）は暗号鍵を用いて計算したMACの一部をペイロードに付与し、データフレームを送信する。監視ノードではCRC※3を照合したのち各送信ノードと同じ暗号鍵を用いてMACを検証する。改良したCANコントローラがなりすましメッセージを検知した場合は、エラーフレームを用いて上書きする。本提案手法は次の2つのフェーズにより成り立っている。

(a) ノード認証と鍵配布のフェーズ
(b) なりすましメッセージのモニタリングとそれをリアルタイムにエラーフレームで上書きするフェーズ

従来研究における手法では、鍵配布のメカニズムは非常に複雑でCANバス上に高い通信負荷をかけるものであり、リアルタイム性が要求される車載制御システムでは受け入れられにくいと考えられる。実車に適用するためには、計算時間の観点から軽量な認証と鍵配送のプロトコルが必要となる。

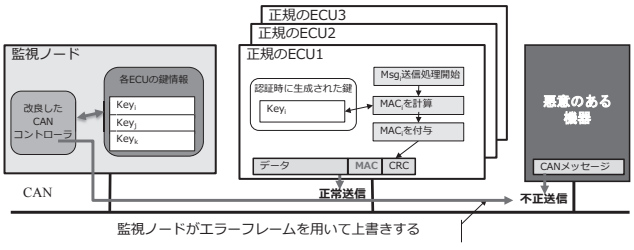

図3　提案手法

3−3　ノードの相互認証と鍵交換

我々が提案するセキュリティ監視システムでは、データフレームのペイロードは暗号化しないため、すべてのノードで同じ暗号鍵を持つ必要はない。それゆえ、我々は監視ノードと各送信ノード（ECU）間の認証にチャレンジレスポンス方式を用いることとした。より具体的には、以下の相互認証のシーケンスを適用する（**図4**）。

1) 監視ノードは送信ノードにランダムシードを送信する。
2) 送信ノードが監視ノードからランダムシードを受け取った後、両ノードはダイジェストの計算を行う。ダイジェストは一般的にハッシュ関数※4によって導出される。

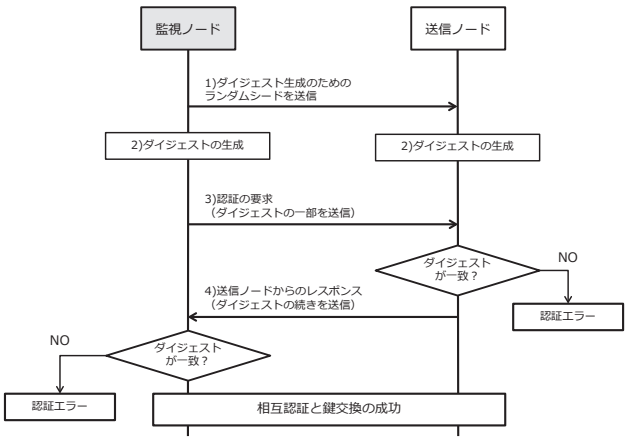

図4　相互認証と鍵交換のプロトコル

3) 監視ノードは送信ノードにダイジェストの一部を送信する。
4) 送信ノードは監視ノードから送付されたダイジェストの一部と自身で計算したダイジェストの比較を行う。一致すれば、続きのダイジェストを監視ノードに送信する。
5) 監視ノードは受信したダイジェストの一部と自身の計算したダイジェストを比較し認証を行う。

3－4　事前共有情報と暗号鍵

本提案手法では、送信ノードには耐タンパ※5メモリが搭載されていないことを想定する。それゆえプログラムコードとユニークIDを含むROMの情報を事前共有鍵として利用することとした。これは監視ノードがすべての送信ノードのプログラムを持つ必要があることを意味する。しかし実際には、監視ノードは予め計算された数種類の認証コードをもつことによりメモリ使用量を減らすことが可能である。また我々は実証においてSHA-256のハッシュ関数を用いたが、これに限定しているわけではない。暗号鍵の詳細を以下に示す。

(a) 事前共有情報

我々の実証では簡単のためプログラムコードを事前共有情報として使用した。それゆえ、認証コードの生成時間はプログラムサイズに依存する。プログラムコードの流出は本方式の欠点となるので、コードの流出による影響を低減する必要がある。そのために実際の環境下では共有情報としてすべてのECUが個々に鍵を持つことを推奨する。

認証コードの生成を下記の**式**に示す。

$$AUTHKEY_I = SHA256\ (MSG\ ||\ NONCE)$$

$AUTHKEY_I$は送信ノードIの認証コードで*SHA256*関数はSHA-256のハッシュ計算の関数である。*MSG*は送信ノードのプログラムコードで*NONCE*はランダムシードとなる。

(b) MAC生成／検証鍵

本提案手法では、MAC生成／検証鍵は、前述の$AUTHKEY_I$の残りを使用することとしている。このため、今回の実装では128ビットのMAC生成鍵を使用することとした。

3－5　認証メッセージ

本提案手法では、メッセージを送信するフレームと認証情報を送信するフレームを分けている。**図5**に一般的なCANメッセージと本提案手法との違いを示す。本提案手法におけるCANメッセージには、ペイロードの一部にMACの一部を付与するが、ペイロードの暗号化は行わないものとする。また**図4**で示した相互認証時には、ペイロード全体に生成されたダイジェストの一部を付与する。

3－6　監視ノードの動作

一般的なCANプロトコルでは伝送エラーを検出するために、すべての受信ノードはCANコントローラを利用してCRCチェックを行う。CANメッセージの完全性を保証するために本提案手法では、**図6**に示すようにペイロードの一部

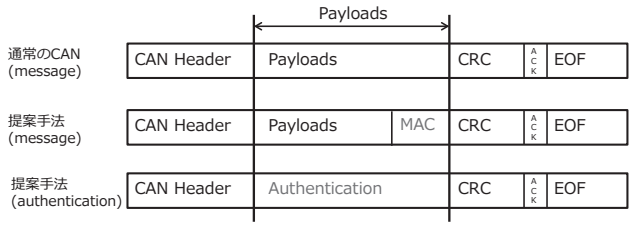

図5　提案手法のCANプロトコル

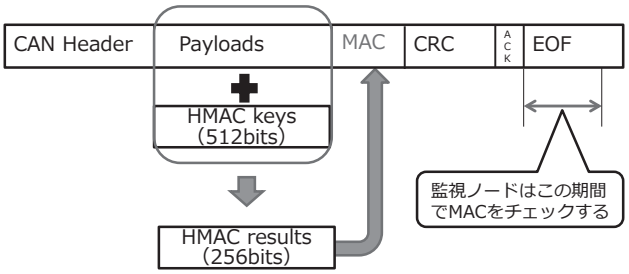

図6　HMACの計算タイミング

にMACを付与する。MACは車載ネットワーク上でのなりすましからデータを保護することを目的とする。本提案手法では実存するCANコントローラとの互換を維持するためにCRCをMACに置き換えることはしない。

監視ノードはメッセージを受信すると、CAN-IDのチェックを行いメッセージにMACが付与されているか否かを判別する。メッセージにMACが付与されている場合には、監視ノードは直ちにHMACの計算を行い、MACの検証を行う。この時点では、どのノードもCANバスにACKを送信していない。しかしながら、監視ノードがMACエラーを検知した場合には、EOF (End Of Frame) までの間に監視ノードがなりすましメッセージをエラーフレームで上書きする。これにより、監視ノードがMACを代理で検証することで、すべての受信ノードでMACを検証することなく、不正なりすましメッセージの送信を阻止することが可能になる。

なお、本提案手法でもペイロードにモノトニックカウンタ※6の一部を付与することで、再送攻撃を防止することも可能になる。

3－7　HMACアルゴリズム

本提案手法では、以下に示すHMAC関数を使用している。

$$CalcMAC_i = HMAC\ (ID_i, D_i, FC_i, Key_i)$$

*HMAC*関数はHMAC-SHA256のようなハッシュ関数である。ID_iはCAN-IDである。Diは受信したペイロードからMAC_iとLC_iを除いた部分、FC_iは完全なモノトニックカウンタである。Key_iは送信ノードiの暗号鍵($AUTHKEY_i$)である。

4. セキュリティとパフォーマンスの分析

4－1 メッセージの完全性

HMACのセキュリティ強度はMAC長が長くなるほど強度があがる。SHA-256を使用するPCなどで利用されるプロトコルでは32バイトのMAC長を利用している。しかしCANのペイロードは最大で8バイトであるのでMACのすべてを1フレームに格納することはできない。我々はMAC長を1バイトと設定することとした。

1バイトのMAC長では特定のメッセージに対する総当たり攻撃は、2^8の回数が必要となる。ランダムな攻撃でなりすましが成功する確率は$1/2^8$であり、これは攻撃が成功するまでに2^8のメッセージを送信する必要があることを意味している。これはセキュリティ上十分とはいえないが、数メッセージを送信した後に鍵をローテーションさせるなどの手法を講じれば、なりすましを行うことは困難になるものと考えられる。

4－2 実時間制約

実時間制約はセキュリティには直接関係しないが、車載制御システムにとっては重要な項目である。

(a) 認証と鍵交換に要するメッセージ数

1つのノードを増やした場合、認証と鍵交換に要するメッセージ数は2増える。1つは監視ノードから送信されるメッセージ（**図4**中の認証の要求）であり1つは追加したノードから送信されるメッセージ（**図4**中の認証のレスポンス）である。このようにメッセージの数は認証を行うノードの数により変動する。メッセージの数は2×n（nは認証を行うノード数）により計算できる。

(b) MACによるオーバヘッド

MAC長はシステム設計者によって決定できるが、我々は1バイトとして計算している。また、再送攻撃防止用のカウンタ長は4ビットであるので全体としては12ビットのオーバヘッドが発生する。これはペイロード全体の19%であり、フレームの拡張識別子（18ビット）の範囲内であるため、実車でも十分に受容可能なオーバヘッドであると考えられる。

5. 提案手法の実装評価結果

先に示したプロトコルとシステムの実証のため、我々はAltera FPGA開発ボードとCANトランシーバボードを使用した。我々のシステムの最大の特徴であるHMAC内蔵CANコントローラをFPGA上に実装した。

使用したFPGA開発ボード（DE2-115 Development and Education Board）は512KbyteのFLASHメモリを持ち、20KbyteのRAMを持っている。**写真1**に実際の評価環境を示す。

この評価環境を用いた計測により、1つの受信フレームのMACを検査する時間はおおよそ2.12μsであることがわかった。CANの転送レートを1Mbpsとした場合において、3ビット時間内に収まっていた。すなわち、CANメッセージのCRCを計算した後で、MAC の検査を開始し、MACを検査しエラーフレームで上書きするために必要な時間である9ビット時間（ACK（2ビット時間）とEOF（7ビット時間）の合計）にエラーフレームの送信が可能であり、十分に実現可能な性能であることがわかった。

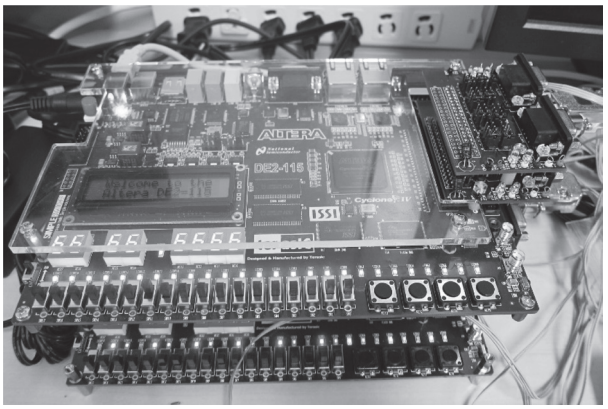

写真1 評価環境

6. 結　　言

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、これまでに様々な車載制御システム向けセキュリティ対策手法が提案されている。しかしながら、それらの手法の多くはすべてのノードに分散して対策が必要になる。本稿では、集中型セキュリティ監視システムを提案し、実証結果についても論じた。

今後は鍵交換などの実証を行い、より車載環境に近い条件において検証を進めていく予定である。

用 語 集

※1　CANコントローラ

CANプロトコルの機能を実現するコントローラ。

※2　メッセージ認証コード（MAC：Message Authentication Code）

通信相手からのメッセージが改ざんされていないことを確かめる認証技術。メッセージの完全性を検証し、認証を行うために用いられる。

※3　CRC

Cyclic Redundancy Checkの略。主にデータ転送などに伴う誤り検出に使用される。異なるデータから同一の値が出力される可能性が常に存在するため、ハッシュ値の代用として使用することは望ましくない。

※4　ハッシュ関数

文字列の羅列から一定長のデータに要約するための関数。関数を通して出力される値は、「ハッシュ値」、または単に「ハッシュ」と呼ぶ。SHA-1やSHA-256といったハッシュ関数が代表的であり、いずれも1方向関数であるため、生成データから原文を推定することは不可能である。

※5　耐タンパ

内部構造や記憶しているデータなどの解析の困難さ。非正規な手段による機密データの読み取りを防ぐ能力を耐タンパ性という。

※6　モノトニックカウンタ

単調に増加していくカウンタのこと。

・FlexRay™は、ドイツDaimler AGのドイツ及びその他の国における商標、または登録商標です。

参 考 文 献

(1) J. Leohold, Communication Requirements for Automotive Systems, 5th IEEE Workshop Factory Communication Systems (2004)
(2) International Organization for Standardization, Road vehicles - Controller area network (CAN) - Part 1: Data link layer and physical signaling, ISO11898-1 (2003)
(3) International Organization for Standardization, Road vehicles - Local Interconnect Network (LIN) - Part 1: General information and use case definition, ISO/DIS 17987-1.
(4) International Organization for Standardization, Road vehicles - Communication on FlexRay - Part 1: General information and use case definition, ISO10681-1 (2010)
(5) K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental Security Analysis of a Modern Automobile, IEEE Symposium on Security and Privacy (2010)
(6) A. V. Herrewege, D. Singelee, I. Verbauwhede, CANAuth - A Simple, Backward Compatible Broadcast Authentication Protocol for CAN bus, Embedded Security in Cars 9th, Dresden, Germany (Nov. 2011)
(7) A. Hazem, Hossam. A. H. Fahm, LCAP - A Lightweight CAN Authentication Protocol for Security In-Vehicle-Networks, Embedded Security in Cars 10th, Berlin, Germany (Nov. 2012)
(8) O. Hartkopp, C. Reuber, R. Schilling, MaCAN - Message Authenticated CAN, Embedded Security in Cars 10th, Berlin, Germany (Nov. 2012)
(9) T. Hoppe, S. Kiltz, J. Dittmann, 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, SAFECOMP '08, pp. 235-248 (2009)
(10) T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, A Method of Preventing Unauthorized Data Transmission in Controller Area Network, Vehicular Technology Conference (VTC Spring) , 2012 IEEE 75th (2012)

執　筆　者

上田　浩史*：㈱オートネットワーク技術研究所
情報ネットワーク研究部　グループ長

倉地　亮*：名古屋大学　大学院情報科学研究科
附属組込みシステム研究センター
特任助教　博士（情報科学）

高田　広章：名古屋大学　大学院情報科学研究科
附属組込みシステム研究センター
センター長　博士（理学）

水谷　友洋：㈱オートネットワーク技術研究所
情報ネットワーク研究部

井上　雅之：㈱オートネットワーク技術研究所
情報ネットワーク研究部　主席

堀端　啓史：㈱オートネットワーク技術研究所
情報ネットワーク研究部　室長

＊主執筆者