不正送信阻止：CAN ではそれが可能である

畑 正人　田邉 正人　吉岡 克成　大石 和臣　松本 勉

横浜国立大学 大学院 環境情報学府・環境情報研究院
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
{hata, masato}@mlab.jks.ynu.ac.jp, {yoshioka, oishi, tsutomu}@ynu.ac.jp

あらまし 現代の自動車は，CAN (Controller Area Network)に代表される車載ネットワークを導入している．CANはバスネットワークを前提としており，やり取りされるメッセージには送信元や宛先ノードの情報が含まれず，同一バス内の全てのノードにブロードキャストされる．また，メッセージ認証や送信元認証機能がないため，容易になりすましが可能である．そこで本論文では，このCANの特徴であるブロードキャスト通信を利用し，不正メッセージがバス上に送信されていることを，なりすましの対象となったノード自身が検知し，エラーメッセージを送ることで，偽装メッセージの送信が完了する前にこれを破棄する“不正送信阻止方式”を提案する．提案方式は，保護対象メッセージの送信ノードに簡易な変更を加えることで実現可能であり，実装上も十分な即時応答性が見込まれるため，CANを利用する車載ネットワークをはじめとする多くの制御系ネットワークシステムへの導入が期待できる．

How to Stop Unauthorized Transmission in Controller Area Network

Masato Hata　Masato Tanabe　Katsunari Yoshioka　Kazuomi Oishi　Tsutomu Matsumoto

Yokohama National University
Graduate School and Research Institute of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama, Kanagawa 240-8501, JAPAN
{hata, masato}@mlab.jks.ynu.ac.jp, {yoshioka, oishi, tsutomu}@ynu.ac.jp

Abstract Modern automobiles utilize in-vehicle networks such as CAN (Controller Area Network). CAN is designed for bus networks, in which transmitted message contains no source or destination information and thus are simply broadcasted to every node in the bus. The protocol has no support for sender authentication or message authentication and is therefore vulnerable to impersonation and spoofing. In this paper, we propose a prevention method for unauthorized message transmission in CAN. The method leverage the fact that every message is delivered to all nodes in the bus network including the one the spoofed message is trying to impersonate. This node detects the spoofed message just in time when it is being transmitted and immediately sends an error message to prevent its transmission. The method can be implemented with minimal changes in the present architecture of Electronic Control Unit (ECU) and can achieve sufficient real-time response. The method utilizes the general characteristics of CAN and therefore could be deployed to not only in-vehicle networks but also other systems that use CAN.

1　はじめに

現代の自動車は，車内の様々な機器の制御を担う ECU (Electronic Control Unit)を多数搭載し，それらを接続する車載ネットワークとして，CAN (Controller Area Network)を導入していることが多い．CAN の導入により高度な制御が行うことができ，セーフティの向上やコスト面などで多くの利点がある．しかし，CANを導入することによる新たな脅威も知られている．例えば，文献[1]では攻撃者が車載ネットワークに直接アクセスできる環境において，ECU の書き換え等の攻撃により，運転者が意図しない動作を発生させられることを実際の自動車を用いて実証している．また，文献[2]では攻撃者が車載ネットワークに直接アクセスできない状況でもオーディオシステムや Bluetooth，携帯電話などを介して侵入することで自動車の制御を乗っ取ることが可能であることが実証されている．文献[3]では，攻撃者がメッセージの挿入を行うことで，パワーウィンドウやエアバック制御システムなどの機能が正常に動作しなくなることをシミュレータやデモシステムで示している．これ以外にも多くの文献で車載ネットワークの脆弱性について言及されており，早急な対応が必要といえる．

自動車は多数の機器からなる複雑なシステムであり，多様なセキュリティ上の課題が考えられるが，最も大きな課題の 1 つに，CANの脆弱性が挙げられる．CANは，バスネットワークを想定しており，やりとりされるメッセージ(CAN ではフレームとよぶ)には送信元や宛先情報が含まれず，メッセージは全てバス上にブロードキャストされる．当該バスに接続されたノード(ECU)は，任意のメッセージを送信することができるため，バス内の ECU が一度不正侵入されると，この ECU が他の重要な制御を行う ECU になりすまして，様々な不正を行うことができる．そこで本稿では，CAN の特徴であるブロードキャスト通信を利用し，不正メッセージがバス上に送信されていることを，なりすましの対象となったノード自身が検知し，エラーメッセージを送ることで，偽装メッセージの送信が完了する前にこれを破棄する“不正送信阻止方式”を提案する．

本稿の構成は以下のとおりである． 2 章で関連研究を紹介する．3 章で CAN について述べ，4 章で CAN における問題点と脅威についてまとめる．その後，5 章で不正送信阻止方式の提案を行い，6 章で考察として評価を行い，そして 7 節でまとめと今後の課題とする．

2 関連研究

これまで多くの先行研究において自動車の車載ネットワークの脆弱性が指摘されている．しかし，これらの脆弱性に対して，車載ネットワークのセキュリティ向上に関する先行研究は多くない．具体的には，通信の内容を暗号化することにより守秘性を実現する手法や認証子や署名を付加することにより認証機能を追加する手法など，暗号技術を用いた保護手法[4 , 5]とIDS (Intrusion Detection System: 侵入検知システム)やファイアウォールにより車載ネットワークを保護する手法[3, 6, 7]に大別される．

暗号技術を用いた保護手法として，文献[4]では共通鍵暗号方式と公開鍵暗号方式を用いることで高速な暗号通信を行う方式を提案している．一方，文献[5]では MAC (Message Authentication Code)を付加し，データフレームの CRC フィールドに格納することでメッセージ認証を行う，Delayed Data Authentication を提案している．

IDS などを導入することによる車載ネットワークの脆弱性を軽減する保護手法として，文献[3]では CAN に導入する IDS において不正メッセージを検知する方法を 3 つ挙げている． また，文献[6]は 9 つの異常検知センサーを定義し，車載ネットワークへの導入を検討している．文献[7]では IDS の検討だけでなく，メッセージ頻度を監視して異常を検知する方式のシミュレーションベースの評価も行っている．

3 CAN (Controller Area Network)

CAN はBOSCH 社によって自動車向けに開発され，ISO11898 およびISO11519 で規格化されている．2 本のワイヤで信号を伝える二線式差動電圧方式を採用しており，ノイズに影響されにくいため，自動車や飛行機，工作機械等の産業ロボットなどで，制御情報の転送を行うシリアル通信プロトコルとして利用されている．各ECU は電位差を変化させることによりデータを信号として送信し，同時に電位差を検出することにより，データを受信する．CANでは，各ECUはバス型ネットワークに接続されており，バス上に流れるデータをすべてのECU が受信できるブロードキャスト通信となっている．

自動車では，CAN の他に LIN (Local Interconnect Network) , MOST (Media Oriented Systems Transport) , FlexRay などが車載ネットワークとして用いられている．CAN は転送速度によって，走行に関する制御を行う高速 CAN とパワーウィンドウなどのボディ系の制御を行う低速 CAN に分けられ，これらが車載ネットワークの基幹となっている(図 1).

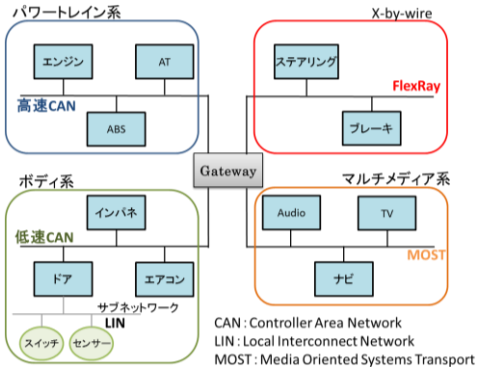

図 1: 車載ネットワークの構成例

3.1 CAN プロトコル

CANにおけるデータの転送は，“0”と“1”の2 進数で行われる．2 本のワイヤの電位差が大きい状態をドミナントと呼び，“0”を表す．逆に電位差が小さい状態をリセッシブと呼び，“1”を表す．複数のECU がドミナントとリセッシブを同時に出力した場合は，ドミナントが優先される仕組みとなっている．

CAN は CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)方式を採用しており，バスに対して最初に送信を開始したECUが送信権を得る．同時に複数のECUが送信を開始した場合，通信調停が行われる．通信調停については，3.2 節で詳しく述べる．

3.2 データフレーム

CANの通信はID フィールドやデータフィールド，CRCシ

ーケンス, EOF などから構成されるフレームという単位で行われる. 特にECU 間のデータの送受信は, データフレームと呼ばれるフレームによって行われる(図2).

データはデータフィールドに格納され, 1 つのデータフレームにより 0~8byte のデータを送信することが可能である. 11bit の ID フィールドは各メッセージの ID を表しており, 加えて, ID は当該メッセージの優先度も表しており, ID が小さいほど優先度は高くなる. 同時に複数の ECU がデータ送信を開始した場合, 通信調停がおこり, ID が小さいメッセージが優先される. 以下で通信調停について詳しく説明する.

ECU がフレーム送信を開始すると, SOF の 1 ビットが送信され, その後, ID フィールドの 1 ビット目が送信される. 複数の ECU が異なるビット値の送信を試みた場合, CAN の物理特性上, ドミナント"0"が優先してバス上に送信される. このとき, リセッシブ"1"を送信しようとした ECU は, 他の ECU が, 自分よりも優先度の高いメッセージを送信しようとしていることを認識できるため, 以降のメッセージ送信を中断する. このようにして通信調停が行われ, もっとも ID が小さいメッセージがバス上に転送される.

図 2:データフレーム

3.3 エラーフレーム

エラーフレームは各ECUが, 送受信中に何らかのエラーを検出した際に, 他のECUへエラーを通知するためのフレームである(図3). エラーフラグとエラーデリミタ, ITM (Intermission)から構成され, エラーを検知したECUがビットスタッフィングルールに違反する形で6bitのドミナント"0"を送信することで開始される. ビットスタッフィングとは, 各ECUがタイミングの同期をとるためのルールで, 同一レベルを5bit連続で送信した場合は反転bitを1bit送信しなければいけない, というCANの仕様である. エラーフレームは, 最初のエラーフラグ(6bit)を受信したECUがスタッフエラーを検出し, エラーフレームの送信を行うことでエラーフラグの重ね合わせが生じる. これによりすべてのECUがエラーの発生を認識し, データ送信中のECUはデータ送信を中止する. その後, 8bitのエラーデリミタと3bitのITMが送信され, バスがデータ送信可能な状態となる.

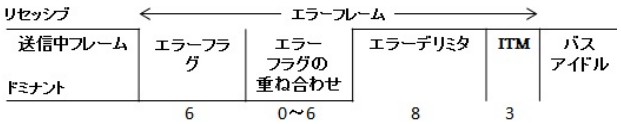

図 3:エラーフレーム

CANプロトコルでは, (a) ビットエラー, (b) スタッフエラー, (c) CRCエラー, (d) フォームエラー, (e) ACKエラーの5つのエラーが定義されており, これらのエラーが検出された場合にエラーフレームが送信される.

3.4 ECU のアーキテクチャ

CANにおける典型的なECUのアーキテクチャは, CPU, CANコントローラ, トランシーバにより構成される(図4). CPUはメッセージの生成や命令の処理などを行う. メッセージの送受信や通信調停などを行うCAN コントローラと CANコントローラからの命令により, CANバスの2本のワイヤの電位差を変化させること及び, 電位差を検出し"0"もしくは"1"の信号としてCANコントローラに渡すトランシーバは, 半導体チップとして実装される.

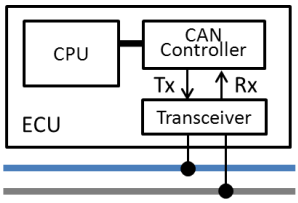

図4:ECUのアーキテクチャ

4 CAN における問題点と脅威

4.1 CAN におけるセキュリティ上の問題

車載ネットワークで用いられているCANプロトコルには, 以下のようなセキュリティ上の問題点が存在する.

- メッセージに送信元情報や認証などのセキュリティ機能が含まれていないため, なりすましが容易に行える.
- バス型であるため, すべてのECUにメッセージが送信される. 従って盗聴や解析などが容易に行える.

既存の研究では, 上記に挙げたような車載ネットワークの脆弱性が指摘されており, それらを悪用することにより 4.2 節で述べる脅威が想定される.

4.2 CAN における脅威

- 盗聴

CAN プロトコルは守秘性がなく, バス型でメッセージがブロードキャストされるため容易に盗聴が可能である. また, OBD-Ⅱポートからある程度のメッセージを受信することが可能である.

- 不正メッセージの送信

OBD-Ⅱポートや不正ECUの接続, 正規ECUの改ざんによりバス上に任意のメッセージを挿入することが可能であるため, 他の ECU になりすまして不正メッセージを送信することができる. 特に, CAN では, 全てのメッセージを観測できるため, 受信した正規メッセージを再度バス上に送信する再

送攻撃が容易に行える.

- DoS (Denial of Service)攻撃

不正ECUによりバスを継続的にドミナント状態にしたり，優先度の高い不正メッセージを連続送信したりすることで，他のメッセージの送信を妨害することが容易に可能である.

上記の脅威の中で，特に，不正メッセージの送信は ECU の誤動作を招き，自動車の走行を危険な状態に陥れるため，その対策は非常に重要である. 本論文では，不正メッセージ送信の対策を検討する.

5 提案:不正送信阻止方式

本章ではCANにおける不正メッセージの送信を防止する方式を提案する. まず準備として5.1節で評価項目，5.2節では前提条件を説明した後，5.3節で提案方式の基本アイディアを示す. 5.4節では提案方式の実装について述べる.

5.1 評価項目

CANにおける不正メッセージ対策の評価項目として以下を設定した.

- 導入コスト

対策の導入に必要なコストは評価項目として当然重要である. 特に，ECUの機能が，対策実現のために変更を強いられる場合はその程度が関心事項となる.

- トラフィック非増加性

CANでは，データ伝送の信頼性の観点からバス占有率に十分な余裕が求められる. 対策の導入によりトラフィックが増加することは望ましくない.

- 検知精度

不正メッセージを正規のメッセージとして見逃す“False Negative”と，正規のメッセージを不正メッセージと誤検知する“False Positive”の両方の誤り率の評価が必要である.

- 即時応答性

不正メッセージを検知した際に，適切な対応を即時に行い，事故などを未然に防ぐことができるかどうかが重要な評価項目となる.

- 規格変更不要性

現行のCANが使われている対象でそのまま広く適用可能な方式を目指すため，CANの規格に適合していることが望ましい.

- ゲートウェイ透過性

送信ECUと受信ECUがゲートウェイを介した異なるネットワーク上に存在する場合がある. このような場合でも適用可能であることが望ましい.

5.2 前提条件

提案方式では各IDのデータフレームを送信するECUはネットワーク上にそれぞれ1つしか存在しないことを前提とする. CANの仕様では，同時に2つのECUが同じIDのデータフレームを送信することを禁止しているため，提案方式の前提条件は現実的である.

5.3 基本アイディア

提案方式は，各ECUがバス上を流れるデータを監視することで不正送信を検知する. すなわち，各ECUは自らが送信するメッセージのIDが，自分以外のECUから送信され，バス上に流れた際に，これを不正メッセージとして検知する. 不正メッセージの送信を検知した場合，当該ECUは即座にエラーフレームの送信を行うことで不正メッセージの送信が完了する以前にこれを中断する. このように，不正に送信されるデータフレームの送信自体を阻止することができる. なお，提案方式はメッセージ送信機能をもつ全てのECUに適用することもできるが，特に重要なメッセージを送るECUにのみ適用することもできる.

5.4 実装

提案方式は不正送信を検知してからそのデータフレームの送信が完了する前にエラーフレームを送信しなければいけないため，物理層に近いレイヤで実装する必要がある. そのため，メッセージの送受信や通信調停などを行うCANコントローラに上記機能を実装する.

まず，対象ECUのCANコントローラの内部に，当該ECUがデータを送信中であることを識別するためのフラグを用意する. フラグのON/OFFのタイミングは以下のようにする(図5).

(0) データ送信前(フラグは立っていない状態)
(1) データフレーム送信開始
(2) データフレームのIDフィールドを正常に送信し終えたらフラグを立てる. 例えばコントロールフィールド送信中にフラグを立てる.
(3) ITMの送信中にフラグを下げる.
(4) (0)に戻る.

次に不正メッセージを検知し，破棄する処理を示す(図6).

(1) 対象となるIDのデータフィールドを受信する.
(2) データフィールド受信中にフラグが立っているか否か確認を行う. フラグが立っていない場合は，即座にエラーフレームを送信する.
(3) (0)に戻る. 対象となるIDのデータフレームを受信するたびに(1)～(2)の処理を行う.

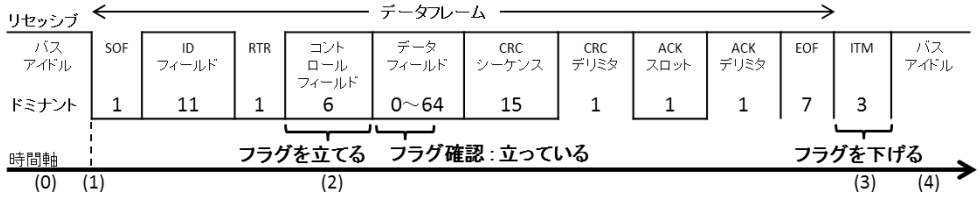

図5：データ送信中を示すフラグのON/OFF

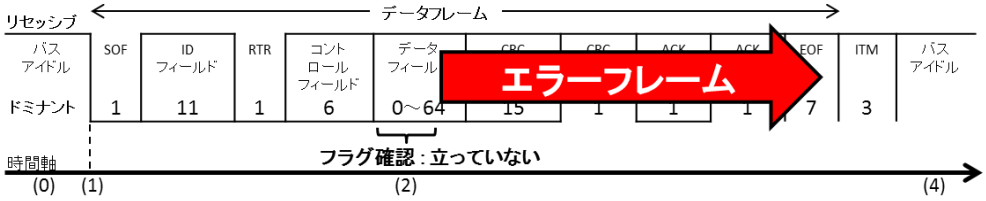

図6：不正メッセージ送信の検知と破棄

6　考察

本章では提案方式の評価と他の保護方式との比較を行う.

6.1　提案方式の定性的評価

● 導入コスト

提案方式はECUのCANコントローラに5.4節に示す簡易な変更を加えることで実現可能である. 特になりすましの影響が大きい重要なECUに対して適用することで小さいコストで大きな効果が期待できる.

● トラフィック非増加性

攻撃が発生していない状況では, 提案方式の導入前と導入後でバスの占有率は変わらない. また, 提案方式では, 不正メッセージ(データフレーム)が途中からエラーフレームとして処理されるため, 攻撃が発生している状況ではトラフィックを減らすことができる.

● 検知精度

提案方式は想定環境において, 不正メッセージを原理的に100%検出することができる. また, 正規ECUが送信したメッセージを不正メッセージとして誤検知することはない.

● 即時応答性

提案方式はCANコントローラへの実装を想定しており, ハードウェア処理されるため, 不正メッセージ送信完了前にこれを破棄することが可能である. つまり, 不正メッセージの送信自体を阻止するので, 不正メッセージによる被害も生じない.

● 規格変更不要性

CANコントローラへのエラー定義の追加のみであり, CANを用いたシステムに広く適用可能である.

● ゲートウェイ透過性

提案方式は, 送信側ECUがデータフレームの送信を行っている途中でエラーフレームの送信を行う必要があるため, フレーム単位で処理が行われるゲートウェイを挟む複数のネットワークには対応できない.

6.2　提案方式の実現可能性

現行のCANプロトコルのCRCエラー処理では, CRCの値の検証を行い, CRCデリミタ直後のビットからエラーフレームの送信が行われる. 提案方式はIDの検出とフラグの確認を行うだけであるため, CRCエラー処理が実現可能なハードウェアと同等のハードウェア上で十分に実現できると考えられる.

また, 一般的にCANではエラー処理をECUのCANコントローラで行っているため, 本稿ではCANコントローラに提案方式を実装することを想定した.

6.3　先行研究との比較

文献[4, 5, 6, 7]で提案されている保護方式に対して, 評価項目における提案方式との比較を行った(図7).

● 導入コスト

IDSを用いた保護方式は, 攻撃検知を行うためのECUを最低1つ追加する必要がある. 一方, 暗号技術を用いた保護方式は, 送信ECUと受信ECUの両者が暗号処理を行う必要があるため, いずれも一定の導入コストが掛かる.
また, IDSを用いた方式は車種ごとにIDSを開発する必要があるが, 提案方式は車種に依存しないため, 開発コストがかからない.

● トラフィック非増加性

提案方式以外の4つの保護方式は, 方式を導入することによるトラフィックの変化はないが提案方式は, 攻撃が発生した場合に不正メッセージを送信完了前に破棄できるため, トラフィックが減らせる点で優れているといえる.

● 検知精度

提案方式と暗号化方式[4]は, すべての不正メッセージを検出でき, 誤って正規のメッセージを不正と判断することも

保護方式		提案方式	暗号技術を用いた保護方式		IDSを用いた保護方式	
評価項目			暗号化[4]	MAC[5]	IDS[6]	IDS[7]
導入コスト	変更を加えるECUの個数	△	×	×	○	○
	ECUを大幅に変更、追加しない	○	△	△	×	×
トラフィック非増加性		○	△	△	△	△
検知精度		○	○	△	×	×
即時応答性		○	×	△	△	△
規格変更不要性		△	×	×	○	○
ゲートウェイ透過性		×	○	○	○	○

図7:先行研究との比較

理論的にはない. MAC方式[5]は正確に不正なメッセージを特定できない. 一方で, IDSでは一般に誤検知と見逃しをなくすことは難しい.

- 即時応答性

暗号化方式[4]は, 不正メッセージを検知してメッセージを破棄することが可能である. MAC方式[5]はメッセージを処理した後に検証を行うため, 不正は検知できるが, 不正なメッセージに基づいて受信ECU上で処理が行われる. 同様にIDSを用いた方式は, 検知用ECUが不正を検知してから何らかの対応を行うまでの間は, 不正なメッセージに基づいて受信ECU上で処理が行われると考えられる.

- 規格変更不要性

IDSを用いた方式は, CANの規格から逸脱しない. 提案方式と暗号技術を用いた方式は, どちらもCANの規格に変更を加える必要があるが, 提案方式はCANコントローラの動作を一部変更するだけであるのに対してMAC方式[5]はCRCをMACに変更しているため, 大きく規格から逸脱している.

- ゲートウェイ透過性

暗号技術を用いた方式はEnd-to-Endで処理を行っており, また, IDSを用いた方式はゲートウェイにIDSを導入することで複数のネットワークに対応できる. しかし提案方式は同一のバスネットワークにおいてのみ有効である.

- その他

暗号技術を用いた保護方式は, 鍵という秘密情報のセキュアな管理が前提であり, 鍵が漏洩したり不正に改変された場合には, 保護方式が破綻する.

7 まとめと今後の課題

本稿では車載ネットワーク等で用いられている CAN において不正なメッセージの送信を阻止する方式を提案した. 不正なデータフレームを検知し, これを上書きするエラーフレームの送信を行うため, 不正に送信されたデータフレームがバス上で受信されないことが特徴である. 従来の保護方式と比べ, 不正なデータフレームの送信自体を中断させることができる点や十分な即時応答性が見込まれる点, 既存のエラー処理と比較しても十分に実現可能であることから車載ネットワークやその他の CAN を利用したシステムへの導入が期待できる.

今後, 本保護方式のシミュレーションベースでの評価やハードウェア実装での評価を行っていく予定である.

参考文献

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental security analysis of a modern automobile,” IEEE Symposium on Security and Privacy 2010, pp. 447 – 462, 2010.

[2] 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,” the 20th USENIX Security Symposium, 2011.

[3] T. Hoppe, S. Kiltz and J. Dittmann, "Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures" In Proceedings of the 27th international conference on Computer Safety, Reliability, and Security, SAFECOMP '08, pp. 235 – 248, 2009.

[4] M. Wolf, A. Weimerskirch, and C. Paar, "Secure In-Vehicle Communication," Embedded Security in Cars – Securing Current and Future Automomotive IT Applications, 2006.

[5] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes," Vehicular Technology Conference VTC 2008, 2008.

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

[7] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying Intrusion Detection to Automotive IT - Early Insights and Remaining Challenge," Journal of Information Assurance and Security (JIAS), pp. 226-235, 2009.