Monthly Research

次世代の車載ネットワークと現状のセキュリティ研究動向

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

はじめに

- 自動車にはエンジンやモーター、ドア、パワーウインドウなど様々な制御を行う為に、多くのECU(Electronic Control Unit)が搭載されていて、これらは車載ネットワーク上で相互に通信を行っている

- レーンキーパーやブレーキアシストなどのドライブアシストシステム(ADAS)やカーナビをはじめとしたIVI(In-Vehicle Infotainment)機器も同様に車載ネットワークに接続されている

- 上述のような自動車に搭載されるデバイス増加とそれらを接続する配線や重量が増加に伴って、低コストかつスケーラビリティのある次世代車載ネットワークに対する関心が高まってきている

- 今回は車載だけにとどまらず、産業用のネットワーク技術として注目されているEthernetと従来の車載ネットワーク(CAN)の問題点や対策例について調査してみた

車載Ethernet

- Ethernetとは、世界中でもっとも普及しているLAN規格の１つで、TCP/IPと組み合わせた通信方法が一般的である
- Ethernetの基本仕様は、OSI参照モデルの物理層とデータリンク層で規定されている（IEEE802.3）
- 近年、自動車メーカーでは新たな車載ネットワークとしてEthernetに関心を持っている
  - 日本ではJasPar※が「次世代高速LANワーキンググループ」としてインフォテイメントデバイスだけでなく制御系デバイス（パワートレインなど）の接続も含めた検討・提案を関連団体に対して行っている
- 家庭やオフィスで一般的に利用されている上述のEthernet規格(100BASE-TX)は環境面において過酷な条件が求められる車載EMI要件を満たしていないことから、自動車での利用は診断やECUファームウェアのアップデート用途が主である

※Japan Automotive Software Platform and Architectureの略

IEEE 802.1 Audio/Video Bridging

- IEEE 802.1 Audio/Video Bridging(以下、Ethernet AVB)は、音声と映像を転送する為の通信規格
- オーディオシステムメーカーや半導体サプライヤーだけでなく、BMWなどの自動車メーカーも参加しているAVnu Allianceが中心になって規格の策定を行っている
- リアルタイム性やフェイルセーフ性が求められる産業/自動車向けにEthernet AVBを拡張した新規格である、IEEE 802.1 TSN(Time Sensitive Networking)の標準化が進められている
- 現行のEthernet AVBに関してもIVI機器に使用するネットワーク向けに国内外の企業で製品開発、発表が行われている

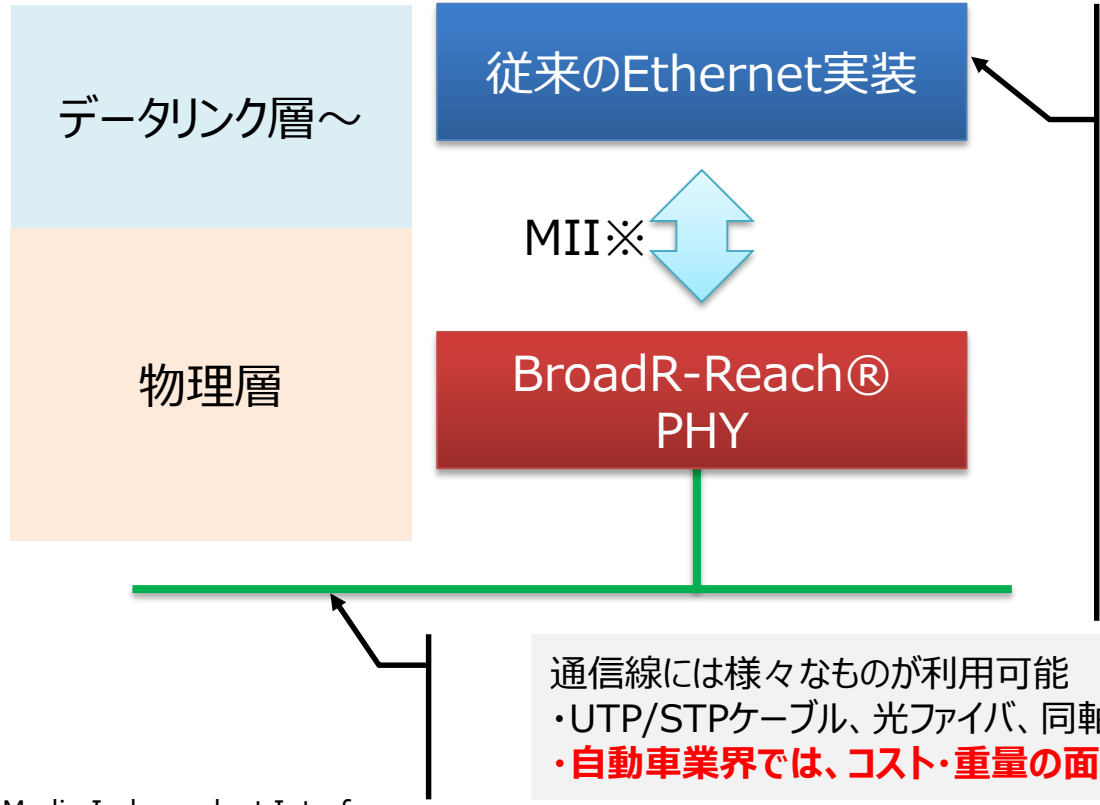
Open Alliance BroadR-Reach

- BroadR-ReachとはBroadcom社が開発し、OPEN Allianceが標準化を後押ししている物理層の技術(以下、OABR)
- この技術では、一部に1000BASE-T(IEEE 802.3ab)の技術を流用することで、従来の100BASE-TXがUTP(Unshielded Twisted-Pair)2対をデータ伝送に使用していたのに対し、1対で全二重の100Mbpsを達成している※
- また、車載Ethernet利用を前提としていることから、この技術を使用したBCM89810ではノイズやジッタに対する信頼性も確保されている
- 一部の自動車では車載カメラを使用したドライブアシスト(ADAS)機能などで既に採用が始まっている

※LANケーブル等で販売、使用されているUTPケーブルは4対/8線で構成される

BroadR-Reach PHY

- Broadcomが開発、販売するBCM89810では、物理層にOABRを採用することでデータリンク層より上位レイヤーは従来のEthernet技術が適用可能



・Ethernet AVB(IEEE 802.1AVB)
・VLAN(IEEE 802.1Q)
・認証(IEEE 802.1X)
・暗号化(IEEE 802.1AE)
・セキュアデバイス(IEEE 802.1AR)
・フロー制御(IEEE 802.3x)
・優先制御(IEEE 802.1p)　など

※BroadR-Reach PHYは物理層を提供し、2-7層は従来のEthernet技術が利用できるが、これらは一例であり、必ずしも車載ネットワークに適用できるとは限らない

通信線には様々なものが利用可能
・UTP/STPケーブル、光ファイバ、同軸 etc・・・
・自動車業界では、コスト・重量の面からUTP(シングルペア)に注目

※Media Independent Interface

車載Ethernetで考えられる脅威の検討

- CAN同様にEthernet(IEEE 802.3)そのものに暗号化など、セキュアな通信を実現する仕組みはなく、セキュリティ関連規格はIEEE 802.1で策定されている
  - ✓ OABRでは物理層が提供されデータリンク層以降はVLANによるネットワークの分離や認証、暗号化といった既存のEthernet技術が利用できるが、メーカーの要求や設計によっては利用されないことも考えられる
- 仕様によってはブロードキャスト型のネットワークになり得ることから、全デバイス宛にフラッディング※したフレームをOBD-IIなどのインタフェースから盗聴することが出来る可能性がある
  - ✓ OABRでは物理層仕様が100BASE-TXや1000BASE-Tとは異なることからパソコンなどに搭載されているNICを使用して車載ネットワークに直接接続する事は容易ではない

- 車載ネットワークがEthernetに置き換わったとしても、原則的な脅威やリスクは従来の車載ネットワークと変わらない（既存ネットワークの脅威についてはp9-11を参照）

- 既存技術の応用であることからITセキュリティとしては一般的であるFuzzingを利用した脆弱性の発見や悪用などの研究が早い段階で行われることが予想される

※L2スイッチやハブでMACアドレステーブルに未登録のフレームやブロードキャストフレームなどを受信した際、全ポートにフレームを転送すること

Ethernetは従来の車載ネットワークに置き換わる？

- 現時点での答えは「NO」
  - 従来のEthernetはメーカーが求める車載要件を満たせていない
    - 車載向けの規格は策定中で未だ承認されていない
  - 次世代の車載ネットワークとして、CANを拡張したCAN FDが提唱されている

- しかし・・・
  - 車載Ethernetは既存技術の応用であるため、伝送速度だけでなくコスト面においてもメリットを受けやすい
  - 家庭やオフィスで使用されているEthernet同様に、車載Ethernetも短期間で大きく成長する可能性がある（IEEE 802.1 TSN, Reduced Pair 1 Gb/s Ethernet）
  - 一部の車種では既にEthernetが部分的に採用されている例もあることから、今後は様々な制御ドメインが徐々にEthernetに置き換わる可能性がある

現状の車載ネットワーク(CAN)に対する脅威

- CAN(Control Area Network)は現在流通している車両でもっとも多く利用され、数年前からセキュリティ上の脅威に関する研究発表が増えている
- CANはブロードキャスト型のプロトコルであり、暗号化も規定されていないことから盗聴が容易である
- OBD-IIに代表される、診断を目的としたCANネットワーク(CANバス)に対してオープンなインタフェースを介してECUに対して任意のパケットをネットワーク上に注入することが出来る
- カーナビなどのIVI機器は車載ネットワークへの接続だけでなく、インターネット接続やモバイルデバイスとの接続を目的に3GやWi-Fi、Bluetoothなどの無線インタフェースを備えているものも多いため、これらのインタフェースを経由した外部ネットワークからCANバスへのアクセスによる脅威が想定される

近年の車載ネットワークに対する脅威報告例（国内）

- 日本国内では、国外に比べてサイバーセキュリティ関連のカンファレンスなどが少なく、アカデミックな分野における論文形式での研究発表が多いのが特徴である

- 2014年のコンピュータセキュリティシンポジウム(CSS)で、横浜国立大学の松本先生らは「電気的データ改ざんに対するCANのインテグリティ強化策」で、CANの仕様上発生し得るデータ改ざんの仕組みとその対策について発表

- 2015年の暗号とセキュリティシンポジウム(SCIS)で、横浜国立大学の松本先生らは「CANにおける再同期を利用した電気的データ改ざん」や日立製作所の森田伸義氏らと「車載ECUに対するCAN経由のファジング手法」について発表

- 2015年の情報セキュリティシステム研究会(ICSS)で、三菱電機の菅原氏らは「強いリセッシブを用いたCANの電気的データ改ざん」で過去に不正送信を防止するために提案されたエラーフレームによる対策を回避する手法について発表

近年の車載ネットワークに対する脅威報告例（国外）

- BlackHat USA ’14でCharlie Miller氏およびChris Valasek氏によって発表された「A Survey of Remote Automotive Attack Surface」では、以下のような指摘がされている
  - 調査した2014年式の車両のうち、42%で少なくとも1つのECUがリモートからの攻撃可能領域との分離が行われていなかった
  - 大部分のコンポーネントが同じバス上にあるなかで、若干の車両は特定の機能を分離していた

- CODEBLUE ’14で岡氏と弊社の松木は、「TriCore車載ECUに対するセキュリティアセスメントの検討と試行」でTriCore搭載機器における理論上の脆弱性分析と攻撃の可能性について紹介
  - TriCoreアーキテクチャにおいても、家庭やオフィスで使用される一般的なx86アーキテクチャなどと同様にメモリ破壊の脆弱性が存在する場合、特定の条件下でCANバスを介して任意のコードを実行できる可能性があることを、意図的に用意した脆弱なソフトウェアを用いた評価ボード上のデモで示した

- BlackHat Asia ’15でEric Evenchick氏は「Hopping On The CAN Bus」でCAN Busに対する攻撃手法やその仕組み、必要なハードウェア、ソフトウェアについて紹介している
  - 容易に行える攻撃手法として、CAN Busに対するDoS攻撃とInjection攻撃を紹介
  - 診断プロトコル(UDS)に対するファジングについても言及

現状の車載ネットワークに対するセキュリティ上の対策例

- エンドポイント対策
  - 特定の条件以外のメッセージは受け付けない（メッセージフィルタ）
  - MAC(Message Authentication Code)認証
    - 近年の論文では、CANの物理層仕様（差動電圧方式による通信）に注目したフレーム改ざん手法などが発表されていることから、CANフレームそのものに対する改ざん検知技術は重要
  - TPMを利用したトラステッドブートによるファームウェア改ざん検知
  - IVI機器に多く搭載される無線インタフェースは、一般的なITセキュリティに基づいた対策(パスワード設定など)を徹底する

- ゲートウェイ対策
  - リモートとの通信インタフェースを持つようなデバイスはゲートウェイ装置によってネットワークを分離、フィルタする

まとめ

- 車載ネットワークに接続されるデバイスやデータ量の増加に比例して重量や材料コストも増加することが懸念されており、これらを解決する技術としてEthernetが注目されている

- Ethernetを採用した場合でも脅威やリスクは原則的に変わらず、既存技術の応用であるぶん、Fuzzingなどを利用して早い段階で様々な検査、攻撃手法について研究されると考えられる

- CANを拡張したCAN FDの存在や、リアルタイム性、フェイルセーフ性などの厳しい車載要件によって、Ethernetが車載ネットワークに対してすぐに置き換わるということは無いといえ、CANをはじめとした既存の車載ネットワークプロトコルに対するセキュリティ研究も引き続き行っていく必要がある

- 近年ではCANの物理層の特性に着目したデータの改ざん手法について国内でいくつか論文発表されており、ファームウェアを初めとしたソフトウェアだけでなく、CANメッセージそのものに対する保護や改ざん検知の仕組みが必要といえる

参考資料

- “車載イーサネット　カーエレクトロニクスの未来と実現へのテスト要件”, イクシアコミュニケーションズ株式会社
  http://www.ixiacom.jp/sites/default/files/915-3510-03-AutomotiveEthernet.pdf
- Dr. Ali Abaye, Richard Barrett, “BROADCOM AUTOMOTIVE NEWS CES 2015 PRE-BRIEFING”, CES2015
  http://www.broadcom.com/docs/press/CES2015_Automotive_prebriefings.pdf
- “車載Ethernetが変える、クルマの未来”, ITPro
  http://itpro.nikkeibp.co.jp/article/COLUMN/20120828/418744/?ST=system
- “車載情報機器向けSoC「R-Carファミリ」から先進運転支援システム（ADAS）に向けた第一弾製品、「R-Car V2H」を発売”, ルネサスエレクトロニクス株式会社
  http://japan.renesas.com/press/news/2014/news20140828.jsp
- “図研エルミックが車載Ethernet用ミドルウェアをルネサスと共同開発 ～ 実用性を高め市場への普及を図る ～”, 図研エルミック株式会社
  http://www.elwsc.co.jp/page.jsp?id=3780
- “Reduced Teisted Pair Gigabit Ethernet PHY Call for Interest”, IEEE 802.3 Ethernet Working Group
  http://www.ieee802.org/3/cfi/0312_1/cfi_0312_1.pdf
- Charlie Miller, Chris Valasek, “A Survey of Remote Automotive Attack Surface”, BlackHat USA 2014
- Takahiro Matsuki, Dennis Kengo Oka, “TriCore車載ECUに対するセキュリティアセスメントの検討と試行” CODEBLUE 2014
- Eric Evenchick, “Hopping On The CAN Bus”, BlackHat Asia 2015
  https://www.blackhat.com/docs/asia-15/materials/asia-15-Evenchick-Hopping-On-The-Can-Bus.pdf
- 松本 勉, 向達 泰希, 土屋 遊, 中山 淑文, 吉岡 克成（横浜国立大学）, “電気的データ改ざんに対するCANのインテグリティ強化策”, CSS2014
- 松本 勉, 中山 淑文, 向達 泰希, 土屋 遊, 吉岡 克成（横浜国立大学）, “CANにおける再同期を利用した電気的データ改ざん”, SCIS2015
- 松本 勉, 小林 優希, 土屋 遊, 吉田 直樹（横浜国立大学）, 森田 伸義, 萱島 信（日立製作所）, “車載ECUに対するCAN経由のファジング手法”, SCIS2015
- 菅原 健, 佐伯 稔, 三澤 学（三菱電機）, “強いリセッシブを用いたCANの電気的データ改ざん”, ICSS
  高田 広章, 松本 勉, “車載組み込みシステムの情報セキュリティ強化に関する提言”
  https://www.ipa.go.jp/files/000034668.pdf
- “2012年度自動車の情報セキュリティ動向に関する調査”, 独立行政法人 情報処理推進機構(IPA)
  http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_report_24.pdf

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research