Monthly Research

Trend of Next-Gen In-Vehicle Network Standard and Current State of Security

F F R I , Inc
http://www.ffri.jp

Background

- Automobiles equip a lot of ECUs which communicate mutually on In-Vehicle Network to control engine, power window, and so on
- IVI devices such as navigation system and ADAS* known-as lane-keeping or brake-assist systems often are connected in the same network
- Because In-Vehicle network becoming complicated by various devices, next-generation In-Vehicle network attracts interest as feasible technology at low cost
- This slide summarized about following topics
  - Ethernet prospective as next-generation In-Vehicle network
  - Recent security research about conventional In-Vehicle network and proposal of measures for the CAN

*Advanced Driver Assistance System

In-Vehicle Ethernet

- Ethernet is a LAN standard spreading most all over the world, and is generally used in combination with TCP/IP
- Basic specifications of Ethernet are prescribed in Physical Layer and Data-link Layer of OSI Reference Model (IEEE 802.3)
- Recently, automobile manufactures are interested in Ethernet as next-gen In-Vehicle network technology
  - In Japan, JasPar* performs study of next-generation network and suggestion to associated group (e.g. The OPEN Alliance)
- However, Ethernet used in home/office does not meet the requirements as In-Vehicle Ethernet

*Japan Automotive Software Platform and Architecture

IEEE 802.1 Audio/Video Bridging

- IEEE 802.1 Audio/Video Bridging (Ethernet AVB) is communication standard to transfer audio and video data
- AVnu Alliance which audio system manufactures and not only semiconductor suppliers but also auto manufactures such as BMW
- Some semiconductor manufactures announce the product in conformity with Ethernet AVB
- Standardization of IEEE 802.1 TSN* which is a next-gen standard for industrial that extended Ethernet AVB is pushed forward

*Time-Sensitive Network

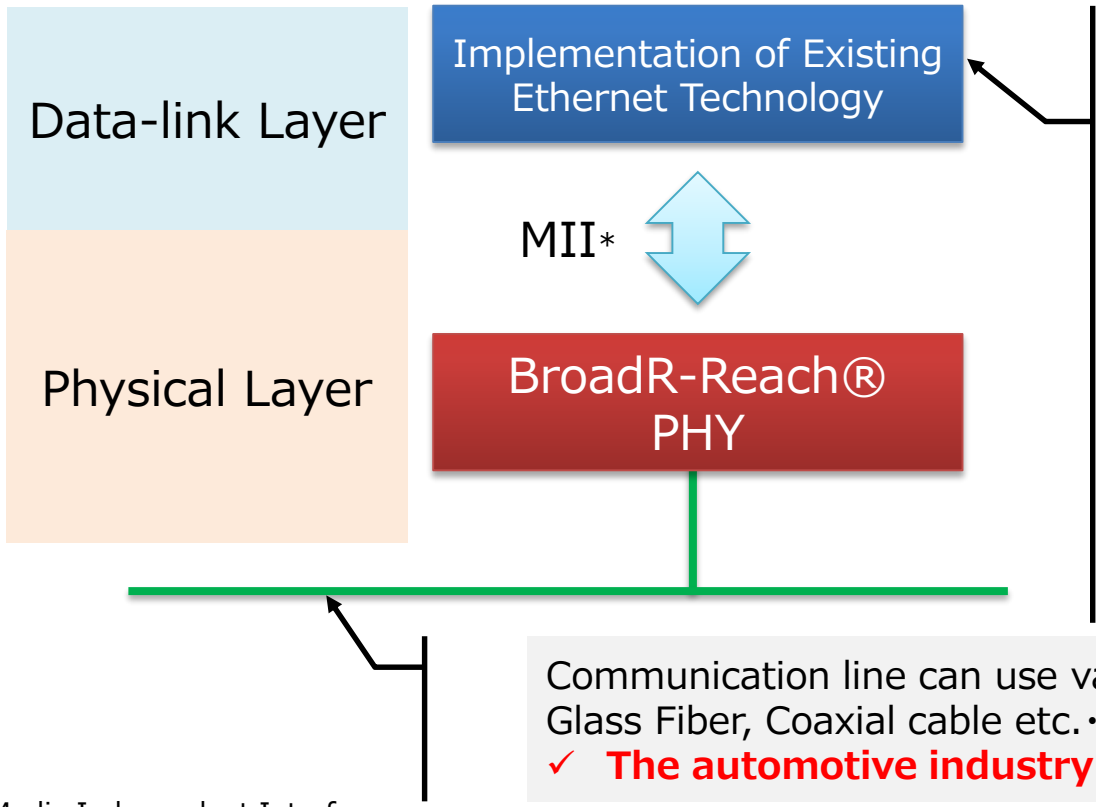
Open Alliance BroadR-Reach

- BroadR-Reach (OABR) is technology of physical layer that Broadcom developed, and OPEN Alliance plays key role to standardization
- This technology achieves 100Mbps/full with one pair whereas conventional 100BASE-TX used UTP (Unshielded Twisted Pair) two pair*1 for data communications by diverting technology of 1000BASE-T (IEEE 802.3 ab) to a part
- In addition, reliability for a noise and jitter is secured in BCM89810*2 using this technology because it is assumed In-Vehicle Ethernet use
- Adoption has already begun by the ADAS using the In-Vehicle camera by some vehicles

*1 UTP cable used in home/office is four pairs (8 lines)
*2 BCM89810 is automotive Ethernet transceiver which Broadcom corp. developed

BroadR-Reach PHY

- In BCM89810, conventional Ethernet technology can apply to layer above the Data-link layer by adopting OABR in physical layer



・Ethernet AVB(IEEE 802.1AVB)
・VLAN(IEEE 802.1Q)
・Authenticate(IEEE 802.1X)
・Encryption(IEEE 802.1AE)
・Secure Device(IEEE 802.1AR)
・Flow Control(IEEE 802.3x)
・Priority Control(IEEE 802.1p)
etc.…

* The BroadR-Reach PHY provides physical layer, and conventional Ethernet technology is available 2-7 levels, but these are an example and may not be necessarily applicable to the In-Vehicle network

Communication line can use various cables(UTP/STP copper, Glass Fiber, Coaxial cable etc.・・・)
✓ **The automotive industry is interested in low-cost UTP**

*Media Independent Interface

Study of Threat Assumed in In-Vehicle Ethernet

- Ethernet (IEEE 802.3) does not have standard to realize encryption and secure communication like CAN, but standard about security is defined in IEEE 802.3

- In-Vehicle Ethernet network may become the broadcast type by network design, and therefore Ethernet frame which did flooding* to all devices may be sniffed on interface such as the OBD-II

- Even if In-Vehicle network was replaced by Ethernet, the topical threats and risks are not changed with exist In-Vehicle network (see also p9-11)

- Because Ethernet is an existing technology, it is easy to perform the penetration test that utilized know-how of IT security (e.g. Fuzzing)

※The situation that a frame is transferred to all ports on L2 switch/HUB when received a frame of non-registration on MAC address table or broadcast frames

The Ethernet replaced by the CAN?

- Currently, the answer is “NO”
  - Existing Ethernet cannot satisfy the In-Vehicle requirement
  - The CAN FD which extended CAN as next-generation In-Vehicle network is proposed
- However…
  - Like Ethernet used in home/office, the In-Vehicle Ethernet may greatly grow up in a short term
  - Because there is the case that Ethernet has been already adopted partially in some vehicles, in future various control domains may be gradually replaced by Ethernet

Threat to current In-Vehicle network (CAN)

- CAN is used for many vehicles now, and the reports about threat in security increase for several years
- CAN is a protocol of the broadcast type, and sniffing is easy because the encryption is not prescribed
- CAN is able to inject any message to ECUs which is on the same network (CAN Bus) from “open interface” such as the OBD-II (In order to use diagnosis)
- Infotainment systems and telematics devices often equip wireless interfaces (e.g. Wi-Fi) and internet connection
  - The threat by access to CAN bus from outside network by way is assumed in these interfaces

Recent reported threat on In-Vehicle network in Japan

- Computer Security Symposium (CSS) 2014
  - Prof. Matsumoto and others of Yokohama National University reported “How to Enhance Integrity of Controller Area Network Against Electrical Data Forgery”

- CODEBLUE 2014
  - Mr. Oka and Mr. Matsuki reported “A security assessment study and trial of TriCore-powered automotive ECUs”

- Information and Communication System Security (ICSS) 2015
  - Mr. Sugawara and others of Mitsubishi Electric Corporation reported “Yet Another Electrical Forgery Attack on CAN using Strong Recessive”

Recent reported threat on In-Vehicle network in International

- Black Hat USA ‘14
  - Mr. Charlie Miller and Mr. Chris Valasek reported “A Survey of Remote Automotive Attack Surface”
    - They said, “6 out of 14 (42%) of the 2014 vehicles we looked at have no separation between at least one cyber physical ECU and one with remote attack surface”

- BlackHat Asia ’15
  - Mr. Eric Evenchick reported “Hopping On The CAN Bus”
    - Introduction DoS and Injection attack for CAN bus as attack technique to be perform easily

Proposed measures for current In-Vehicle network security

- Endpoint
  - Message filtering
  - Adoption of MAC(Message Authentication Code)
  - Firmware manipulation detection by the Trusted Boot using TPM
  - Thorough general IT security measures (e.g. complicated password settings)

- Gateway
  - Separation of the In-Vehicle network
  - Limit to access to specific ECUs

Wrap up

- Because In-Vehicle network becoming complicated by various devices, Ethernet attracts attention as a technology to solve
- The next-generation In-Vehicle network is expected in various factors, but topical threat does not change with conventional CAN network
- In-Vehicle network is not replaced by Ethernet immediately
  - It should continue studying the threat of conventional CAN network
- Recently, some researcher reported about the manipulation technique of CAN message
  - Measures for the CAN message itself are important (e.g. MAC authentication)

References

- “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
  http://www.ffri.jp/research/research_papers.htm
- 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
- 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