In-Vehicle Networks Outlook: Achievements and Challenges

Weiying Zeng, *Student Member, IEEE*, Mohammed A. S. Khalid, *Member, IEEE*, and Sazzadur Chowdhury, *Member, IEEE*

***Abstract*—This paper presents a comprehensive survey of five most widely used in-vehicle networks from three perspectives: system cost, data transmission capacity, and fault-tolerance capability. The paper reviews the pros and cons of each network, and identifies possible approaches to improve the quality of service (QoS). In addition, two classifications of automotive gateways have been presented along with a brief discussion about constructing a comprehensive in-vehicle communication system with different networks and automotive gateways. Furthermore, security threats to in-vehicle networks are briefly discussed, along with the corresponding protective methods. The survey concludes with highlighting the trends in future development of in-vehicle network technology and a proposal of a topology of the next generation in-vehicle network.**

***Index Terms*—In-vehicle network, system cost, transmission capacity, fault-tolerance, automotive gateways.**

I. Introduction

ENCODED communication channels have long been used to transmit signals among different controllers in in-vehicle networks. The typical motivations behind this fact are: 1) Reducing cable cost: Wire harness system is the third most expensive and heaviest system in a vehicle after engine and chassis [1]. In order to lower the production cost and increase fuel economy, using coded communication lines is a good strategy to follow. 2) Saving packaging space: As vehicles tend to get smaller in size, but more enriched in E/E (Electrical and Electronic) features, routing of wire harness has become increasingly challenging. Meanwhile, since cables are potential victims of electromagnetic interference as well as sources of heat, packaging issue is never negligible [2], [3]. 3) Catering to the demands for higher bandwidth: Currently, some high-end passenger vehicles, even not fully featured, already have approximately 70 ECUs (Electronic Control Units) with 2500 signals to transmit internally [4]. In addition, the bandwidth demands from ADAS (Advanced Driver Assistance System) and many other sophisticated applications are constantly rising. It is only possible to facilitate such vast data exchange using encoded communication. 4) Enhancing communication reliability: Digital transmission has unparalleled advantages in terms of signal integrity and robustness than the traditional point-to-point analog wires [5]. Moreover, digital signals also allow encryption to further enhance data security for in-vehicle communications.

There are five most widely used in-vehicle networks in modern intra-vehicle communication systems: LIN (Local Interconnection Network), CAN (Controller Area Network), FlexRay, Ethernet, and MOST (Media Oriented Systems Transport). Each has its own competitive advantages over others, but also has some shortcomings that hinder it from overwhelming any other as well.

From real-world observations, LIN is often used in low speed communications which usually do not require stringent timing performance. CAN is widely deployed in powertrain and body control domains, as well as being a standard interface to retrieve OBD (On-Board Diagnostics) data from vehicles. FlexRay has high determinism and fault-tolerance, which are usually required in applications such as advanced chassis control and communication backbones. Wired Ethernet is still relatively new in series production cars and may have only been used in applications such as ECU flashing and limited network backbone connections. However, it has great potential for high speed data transfer with very limited latency and jitter. Thus, Ethernet may acquire more share of in-vehicle networks in the future. MOST network is primarily deployed as the carrier of infotainment data, which usually demand very high bandwidth and are more common in premium vehicles.

There are some other contemporary communication networks being used in vehicles as well, such as VAN (Vehicle Area Network), TTCAN (Time-Triggered CAN), CANFD (CAN with Flexible Data-Rate) and LVDS (Low-Voltage Differential Signaling). However, they are either experiencing dwindling popularity or have not been widely adopted by auto industry yet at the time of this survey. For instance, VAN was once very popular especially among French automakers, but is now being phased out because of less desirable bandwidth (just up to 125K bit/s) and inferior clock recovery capabilities (less frequent transmission may make clock recovery harder). TTCAN could add deterministic feature to CAN networks, but has not been quite popular in production cars yet, since OEMs (Original Equipment Manufacturers) may directly move to FlexRay, which could provide both greater bandwidth and fault-tolerance than TTCAN. CANFD is a newly standardized protocol and a cost-saving upgrade of traditional CAN. Although it could transmit a payload of 64 bytes at a much faster speed, only a few automakers have implemented it on very limited number of projects to date. The primary reason is that it cannot realize high bandwidth and determinism

Manuscript received February 3, 2015; revised July 26, 2015 and December 1, 2015; accepted January 11, 2016. Date of publication January 27, 2016; date of current version August 19, 2016. This work was supported in part by NSERC, in part by Ontario Centres of Excellence (OCE), in part by CMC Microsystems, and in part by AUTO21.

The authors are with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada (e-mail: zengw@uwindsor.ca; mkhalid@uwindsor.ca; sazzadur@uwindsor.ca).

Digital Object Identifier 10.1109/COMST.2016.2521642

simultaneously. LVDS is mostly used to transfer high speed audio/video data. However, with more inexpensive alternatives, such as Ethernet, coming into play, LVDS is losing its importance in the automotive market [6], [7]. Considering the aforementioned scenarios, networks such as VAN, TTCAN, CANFD and LVDS are not discussed in detail in this paper.

As in-vehicle networks grow fast in size and complexity, problems such as software heterogeneity and reusability have also quickly emerged. Middleware technology has subsequently been widely used by the automotive industry to eliminate software heterogeneity and facilitate software integration of in-vehicle networks. It is an approach to insert an additional software layer between ECU application and the application layer in the OSI (Open Systems Interconnection) model [8]. Currently, the main available middleware include: OSEK/VDX (Open System and the Corresponding Interfaces for Automotive Electronics/Vehicle Distributed eXecutive) [9], Volcano [10], and AUTOSAR (AUTomotive Open System ARchitecture) [11]. In practice, middleware layer can also be used to ensure QoS properties of communication system, such as correcting inconsistent message duplication [12].

This survey paper differs from the previous publications such as [13]–[17] as follows: First, it provides a comprehensive review of different in-vehicle networks from three of the most critical perspectives: system cost, transmission capability, and fault-tolerant abilities. Second, it also identifies possible methods to improve the QoS of each network (such as ensuring bounded end-to-end delay, deterministic transmission, and reliable data delivery). Third, software implementation of each network is discussed with reference to the OSI model. Fourth, two classifications of gateways have also been presented. Fifth, the typical security threats to in-vehicle networks and possible protective measures against the backdrop of autonomous and cooperative driving are discussed. This work aims to serve not only as a review of the state-of-the-art in-vehicle networks for readers with different backgrounds, but also a practical guide for constructing an in-vehicle communication system using one or more of the network technologies discussed in this paper.

Based on our research and real-world experience, we conjecture that all the currently-used major in-vehicle networks will still have great influence in the near future. However, Ethernet may have more significant growth than others. It may also expand to many traditionally non-Ethernet fields in vehicles rapidly. Furthermore, domain specific (or zone oriented) E/E architecture will become even more popular than before. As the complexity of E/E systems grows, the ECUs that interact most closely with each other will be encapsulated in the same domain and separated from other parts of the network by gateways (or domain masters). Network backbones between different domains need meticulous design to meet the requirements of controlled signal latency and jitter.

The remainder of this paper is organized as the follows: Section II to Section VI present an extensive review of LIN, CAN, FlexRay, Ethernet, and MOST networks from three crucial perspectives. Specifically, cost analysis is conducted from system composition aspect with quantitative estimations provided; transmission capability is mainly studied in terms of bandwidth and protocol efficiency; fault-tolerant capability is investigated primarily through the metrics such as Hamming Distance (HD) and Bit Error Rate (BER). Two classifications of automotive gateways and an exemplary in-vehicle network topology are presented in Section VII. In Section VIII, the security threats to in-vehicle networks and the most commonly adopted protection approaches are discussed. Section IX concludes the review with discussions about the considerations of choosing different networks and the future trends of next-generation in-vehicle networks.

II. LIN Network

LIN is a low-cost, low-speed and easy-to-implement in-vehicle network, which has mostly been used in the simple and less time-critical applications, such as traditional central door lock activation, window lifter control, mirror adjustment, steering wheel button module, and many low refresh rate sensors.

A. LIN Cost Analysis

The most prominent advantage of LIN is that it has much lower cost than other major networks [18]. This advantage comes from a variety of aspects. Firstly, LIN controller is relatively cheaper. LIN modules use UART (Universal Asynchronous Receiver/Transmitter) ports to transmit and receive serial data. Since UART ports are available on almost all microcontrollers, even the cheapest microchip may serve as a LIN controller. Secondly, the physical communication cable of LIN costs much less. A LIN station just needs one unshielded signal line to transmit data, and other stations only need to measure the voltage on that line with respect to their own grounds without the need of an additional reference cable. Thirdly, a LIN software stack is relatively easier to develop than other major in-vehicle networks, and it only requires limited space in memory. For instance, the software stack of a typical LIN 2.2 master node is just around 3K to 5K bytes, which is minor compared to the memory available on most automotive class MCUs (Microcontroller Units). Since LIN controllers are already available on virtually all the MCUs, it usually requires only 1~2 US dollars investment on the transceivers and cables to build a simplest LIN network

Currently, LIN is still so broadly used in automotive networks primarily because of its unparalleled cost competitiveness. It is common today that a premium car has more than 30 LIN nodes if fully loaded.

B. LIN Transmission Capability

LIN network is constructed mostly in linear bus topology and operates in a master-slave pattern. Slave nodes synchronize themselves with the master at every transmission of the message header, and remain synchronized within the required bit rate tolerance throughout the rest of that frame.

There is only a single master node, and up to 15 slave nodes in a LIN network. Different nodes gain access to the network based on the schedule table, which is stored in the master node. The bus length of a LIN network should not exceed 40 meters

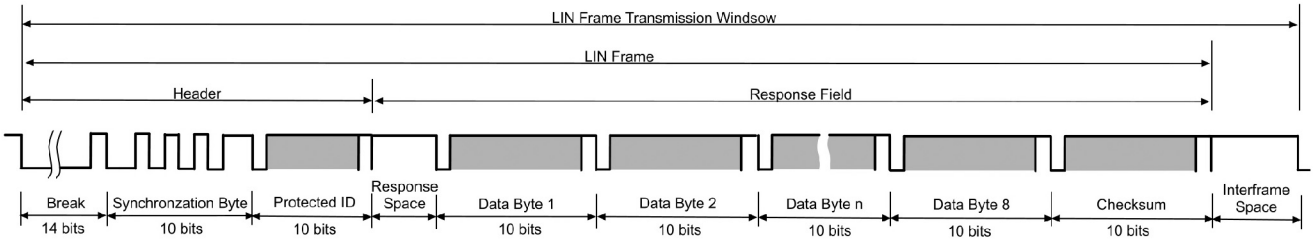


Fig. 1. The structure of LIN frame.

(recommended value), and the total number of nodes should be no more than 16 [19].

In reference to OSI model, only three layers (physical layer, data link layer, and application layer) are needed to realize single-frame on-board LIN communication [20].

Maximum protocol efficiency M is an indicator of the maximum percentage of a message frame that can be used to transfer application data. It is defined as the following:

$$M = \frac{P}{L} \times 100\% \tag{1}$$

where P is the maximum payload of the frame, and L is the corresponding length of the complete frame. As shown in Fig. 1, the maximum payload of a LIN frame is 64 bits and the length of such a frame is 124 bits, thus the maximum protocol efficiency of LIN is 51.6%.

Considering the commonly used baud rate 19.6 Kbit/s in automotive LIN networks, the theoretical limit of LIN payload is 10.12 Kbit/s. In reality, however, this limit may not be fully exploited for a number of reasons, such as wasted bandwidth and up to 40% bit time tolerance. As a consequence, LIN is not suitable for time-critical communications, although the transmission of LIN frames are virtually collision free [21].

C. LIN Fault-Tolerance Capability

LIN adopts One's Complement Addition Checksum to detect transmission errors, which is realized by inverting the eight bits sum with the carry-out bit added at the back of the checksum [19]. This checksum mechanism has a Hamming Distance of 2, and is more capable in detecting msb (most significant bit) errors than Integer Addition Checksum mechanism. However, it still cannot detect compensating errors, and is not data independent either [22]. Analysis has shown that in the worst case this checksum algorithm could have an undetected two-bit error rate in LIN communication at approximately 1/16, which is fairly poor for any safety related applications [23].

In addition to checksum, LIN also has some other mechanisms for error detection. For instance, parity bit can help filter out exotic headers; read back mismatch monitoring could trigger abortion of the incorrect transmission; response error bit is useful to report received or transmitted errors in the response field.

Though LIN network only has limited capability in fault-tolerance compared to other major in-vehicle networks, its polling transmission mechanism can effectively eliminate message collision and arbitration delay. This mechanism may be adopted by other networks to enhance their determinism.

III. CAN Network

CAN network has long been used to transmit the majority of in-vehicle communication signals. Although various different networks have been developed afterwards in response to some requirements that CAN does not meet, CAN still retains the popularity in automotive networks, particularly in powertrain system and upper body electronics. The estimated number of CAN chips in vehicles has reached nearly 500 million. A recent forecast even expects CAN network will keep thriving in in-vehicle communication systems for the next ten years [24].

A. CAN Cost Analysis

One important reason behind the continuing popularity of CAN protocol is its relatively low cost. Some pundits argue that it only needs 3 US dollars extra to make an existing microcontroller CAN-equipped [25]. As more and more energy efficient and electromagnetically sophisticated CAN transceivers being introduced to the market, the marginal hardware cost of a CAN network is dropping very fast.

Another noticeable reason is the mature full-scale tool chains of CAN system, from data dictionary design to production code automatic generation, from network simulation to software validation. These all help to lower the engineering cost of a CAN system significantly. Industry leaders such as Vector Informatik GmbH, Mentor Graphics Corp., and KPIT Technologies Ltd are all capable of supplying reliable CAN embedded software.

Although not intended just for CAN, AUTOSAR is also a significant practice to slash down CAN system cost. AUTOSAR advocates better management of the growing E/E complexity by standardizing the interfaces and increasing interchangeability and reusability of both hardware and software components. Consequently, this would reduce the cost of software integration and tests noticeably.

Since most automotive class MCUs have already equipped with CAN controllers, oftentimes it only needs to invest on the transceivers and cables to make an existing network CAN-supported. For a simplest two-node CAN network with sleep mode supported transceivers, the cost today is roughly 2~3 US dollars.

B. CAN Transmission Capability

CAN network may come with various topologies depending on different physical layers it adopts. For instance, the most widely used CAN network is high speed CAN (baud rate higher than 125 Kbit/s), which is often constructed in linear bus

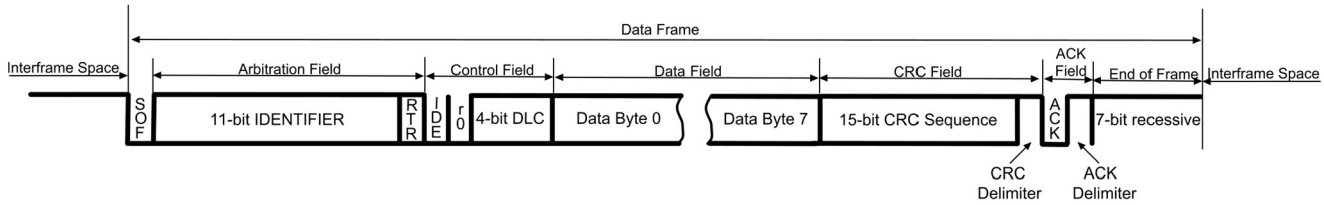


Fig. 2. The structure of standard CAN data frame.

topology and characterized by two 120 Ω terminal resistances at the end of the transmission cable [26], [27]. The less popular low-speed fault-tolerant CAN may be connected in either linear bus or star topology, and is characterized by a baud rate between 40 Kbit/s to 125 Kbit/s with distributed terminal resistors virtually in all nodes [28]. Single-wire CAN is primarily used by GM (General Motors). It supports both ring and star topologies at a baud rate of 33.3 Kbit/s with 9.09 KΩ resistance in the terminal nodes [29].

When mapping to OSI model, CAN network only requires layer one, two and seven for on-board communication (except diagnostics) [20]. These layers correspond to physical layer, data link layer, and application layer, respectively.

An advantage of CAN network is that it does not require any global timer nor centralized coordinator to regulate the communication. Individual node synchronizes its time with the talker when receiving messages. Conventionally, CAN nodes access the network on event-triggered basis, which means every node has the equal right to try to access the bus when the transmission event is ready and the bus is idle. But when multiple nodes initiate attempts at the same time, they need to compete for the access through a non-destructible CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) scheme [30], the lower the message ID the higher the priority to transmit.

This type of MAC (Media Access Control) brings great flexibility in network design, but also brings in big problems when stringent determinism is demanded as in the safety-related applications [15], [31].

As stated in [26] the maximum bus length is 40 m with a minimum node distance of 0.1 m (@1 Mbit/s). The maximum number of nodes is determined by multiple factors such as baud rate, transmission media, CAN driver, and the requirements of a particular application. The fundamental rule is that every two nodes in the same network section should be able to sample the same bit value, considering propagation delay. Some practical insights about how to determine the minimum distance between CAN bus nodes have been presented in [32].

Due to the non-deterministic nature of CAN protocol, in real practice people often focus more on the bus load to determine how many nodes (or messages) can be allocated to one network rather than actually compute the minimum distance between two nodes in that network section. For instance, some scholars in [31] believe only 50% of full bandwidth can be exploited for high speed network, while it is also claimed in [33] that a utilization rate of more than 60% is seldom adopted despite being theoretically feasible. However, based on the real-world observations, most in-vehicle high speed CAN buses just have a load around 30%-33% in order to offset indeterminism in extreme cases.

The most commonly used frame in in-vehicle CAN network is standard frame. Its structure is shown in Fig. 2, where the maximum payload is 64 bits and corresponding frame length is 108 bits. According to (1), the maximum protocol efficiency of a CAN data frame is 59.26%.

However, this is only true in theory when data bytes are maximized and stuff bits are excluded. Considering the commonly used 500 Kbit/s baud rate, the maximum useful data bandwidth of a CAN bus is around 296 Kbit/s (without considering interframe space). In addition, message IDs, if well designed, can also carry some meaningful data other than just be used for arbitration. However, this is a data rate that can never be reached in real-world automotive CAN bus, because bus load often needs to be much lower to offset indeterminism and accommodate diagnostic frames. This is also an unreachable ceiling for TTCAN [34], since it naturally has higher protocol overhead than traditional CAN. Nevertheless, the newly standardized CANFD [35] bears the potential to break this efficiency limit quite a lot, as it supports a payload up to 64 bytes, and may also take part in standard CAN communication.

C. CAN Fault-Tolerance Capability

Another reason for CAN's dominance in the past years is its acceptable capabilities of noise-resistance and fault-tolerance.

CAN network uses unshielded twisted pair (UTP) which has higher resistance to external common-mode interference than untwisted cables such as those in LIN network. Also, they can lower the radiation of high-frequency noises [31]. Additionally, most CAN transceivers today provide extra means to detect and report different kinds of physical layer failures. They are helpful in maintaining robust operation of the network.

CAN protocol in general provides a fairly high level of error detection through a variety of methods, such as transmitter self-checking (bit error and acknowledgement error), receiver cross-checking (cyclic redundancy check error) and double-side checking (stuff error and format error). The total probability of undetected incorrect message is less than Message Error Rate (MER) $\times 4.7 \times 10^{-11}$ [19].

The HD of CAN CRC (Cyclic Redundancy Check) is 6, which means all random errors up to 5 bits in the protected section are detectable. In spite of higher computational overhead compared to many other mechanisms, CRC is still proven effective in achieving a high level of error detection [36].

If a CAN node detects a protocol error, it signals all other nodes in the same network section by an error flag. A CAN station is able to withhold unnecessary reactions to short time disturbances by the Error Counter scheme, when the number of accumulated errors is lower than an acceptable threshold. It

could also release the network for a short period through Bus-Off mechanism when the transmit error counter has reached 256.

Admittedly, CAN is the de facto dominant automotive network, but it still has some critical drawbacks, especially for high safety applications.

Indeterminism is an inevitable problem of conventional CAN due to the nature of its arbitration mechanism. In such a mechanism, the lowest ID will always win access to the network, and the other messages will have to wait for the bus to become idle even when they contain more urgent signals. To solve this problem some TDMA (Time Division Multiple Access) protocols have been introduced, such as TTCAN [34]. In addition, a novel mechanism that has better multichannel clock synchronization than TTCAN is presented in [37], which could maintain highly reliable communication by introducing duplicated channels.

There are some efforts to ease indeterminism within the scope of traditional CAN as well. For instance, indeterminism can be mitigated through meticulous calculation of response time and period of all messages [38]. The commercially available Volcano Network Architect (VNA) [39], [40] is a real practice of this idea and could generate communication matrix based on thorough consideration of signal timing requirements [10], [41]. As proved in [42], schedulability can be enhanced through the proposed UST (Unfixed Start Time) algorithm to better suite real-time applications.

Byzantine General Problem [43] is another critical problem of CAN network, and many other networks. The problem is that how the sender and receiver can reach mutual consensus on the integrity and authenticity of the messages transmitted in between. Since the acknowledgement in CAN network does not signify which node it comes from, the publisher cannot always ensure its message has been correctly received by all the designated nodes in the same (sub)network. For instance, if a node is erroneously offline, it would not even be able to send out an acknowledgement back to the publisher, while the publisher may not notice that if any other node has correctly acknowledged the message. Furthermore, the unprotected sixth bit of End-of-Frame (EOF) may cause inconsistency among different nodes [44], because the receiver only checks form error up to the sixth bit of EOF field and leaves the seventh bit "don't care". For instance, if one receiving node detects an error locally at the sixth bit, it would discard the message and transmit error flag starting from the seventh bit, whereas other receiving nodes may not be aware of the error and still deem the previous message as correctly received. Consequently, data inconsistency is created.

CAN also lacks means to handle Idiot Bubbling Failure. A bubbling idiot station (with a sufficiently low ID) may trash the whole network by repeatedly sending garbage messages too frequently and suppress normal communication between other stations. As a countermeasure, Bus Guardian Mechanism has been introduced later on to tackle this problem. A typical bus guardian, such as the design in [45], works in Wire-AND logic so as to mute the bubbling node. There are also some alternatives such as 'pipelined forwarding distribution method' proposed in [46], though subject to some other restrictions. For instance, certain bits of message ID need to be reserved, and no bit stuffing is allowed in the arbitration field.

Moreover, middleware technology such as SOAcom [47] can also help develop service-based Driver Assistance Systems (DAS) on CAN network. Real-time guarantee and fault-tolerance features can be realized by the middleware structure proposed in [48] as well.

In practice some additional approaches can also be adopted to improve QoS of CAN network, such as: assign a lower ID and set the critical message as 'event-triggered' or 'mixed' transmission type other than 'purely periodic' to shorten end-to-end latency; bus-off before error counter reaches 256 to increase node sensitivity to bus errors; introduce network management mechanism to ease Byzantine General Problem, etc.

IV. FlexRay Network

Motivated by the goals of tackling indeterminism, increasing bandwidth, and enhancing fault-resistance of networks such as LIN and CAN, FlexRay is evented by FlexRay consortium [49]. Presently it has been growingly adopted in vehicle dynamics domain and inter-domain communications.

A. FlexRay Cost Analysis

FlexRay network has much faster transmission speed and greater fault-tolerance than LIN and CAN. It also has significantly higher cost, although the actual cost of a FlexRay system may be controversial.

For example, some experts think the cost of FlexRay is just too high, and worry this might deter its broad acceptance by the automotive industry [18], [50], [51]. Some also believe FlexRay would have very limited future because it is too complicated to be deployed in vehicles [52]. But as per [53], FlexRay would have approximately the same cost as a CAN system, considering that it can replace multiple CAN subnetworks and some redundant sensors.

From system composition perspective, FlexRay, though, uses the same transmission media as CAN, it usually requires twice redundancy of the cables and transceivers than CAN in order to achieve high fault-tolerance. Hence, even for a simplest FlexRay network with only two nodes, there will be four transceivers and two separately routed transmission cables, which altogether may cost 12~14 US dollars, not to mention the engineering complexity in coordinating between the two independent channels.

Based on the arguments above, FlexRay is still expensive at present, considering both hardware cost (e.g., two independent channels) and engineering efforts (e.g., more than 80 parameters to configure [54]).

However, if the FlexRay equipped X-by-Wire system (such as Steer-by-Wire or Brake-by-Wire system) could completely replace the traditionally cumbersome mechanical parts (such as steering column or hydraulic brake channels), it may be one of the most cost-saving networks in automotive applications in the future.

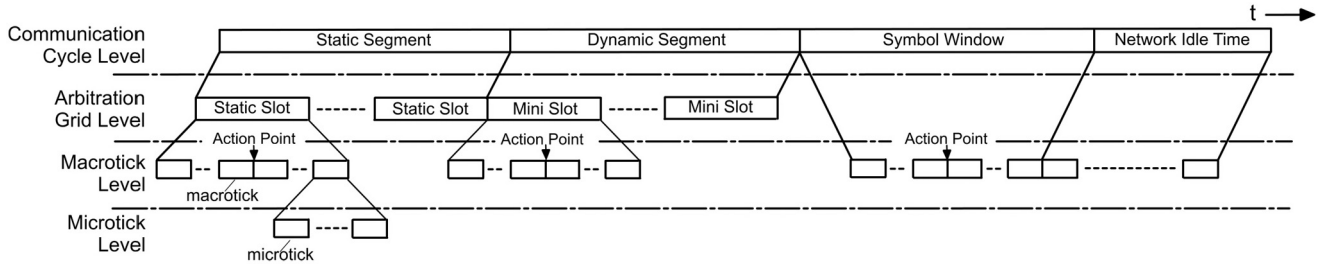


Fig. 3. Time hierarchy of a FlexRay communication cycle [39].

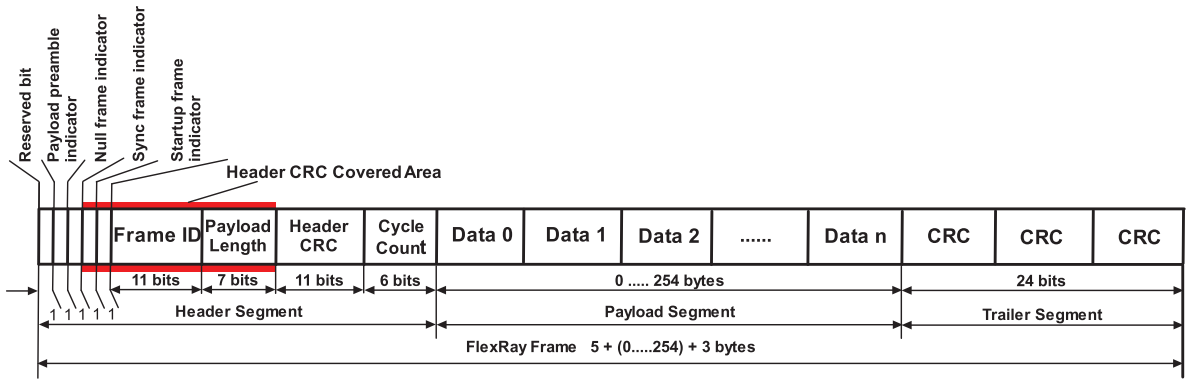


Fig. 4. FlexRay frame format.

B. FlexRay Transmission Capacity

Unlike other automotive buses, FlexRay has two parallel channels each up to 10 Mbit/s (designers can choose among 10 Mbit/s, 5 Mbit/s, and 2.5 Mbit/s baud rate [55]). The additional channel is designed to be a backup in case of any communication failure in the other. However, due to the independence of the two channels, it is not always necessary for both channels to transmit the same data, which virtually gives FlexRay 20 Mbit/s transmission bandwidth in extreme (at the expense of redundancy loss). Similar to LIN and CAN, FlexRay network typically needs only physical layer, data link layer, and application layer in reference to OSI model for on-board communication [20].

There are three most prominent properties regarding FlexRay's transmission capabilities: 1) it can transmit both deterministic and dynamic data in the same cycle; 2) it has much greater payload than LIN and CAN (including TTCAN and CANFD); 3) it is very flexible in terms of network topologies.

Partly as an invention to meet the rising demand for deterministic transmission of safety related applications, FlexRay incorporates the transmission of time-critical messages together with the event-driven ones. As shown in Fig. 3, a transmission cycle is divided into separated slots, which are in line with the synchronized global time among all network participants. In one slot of a specific cycle, only the message meeting a specific ID requirement has the right to access the bus. Consequently, the static segment is suitable for transmitting messages with time-critical data, such as the signals for vehicle safety and driving dynamics controls. Since only the designated ID has the right to transmit in a fixed slot, the sender does not need to worry about the arbitration delay on the bus. The dynamic segment, on the other hand, has inherited the essence of ID priority arbitration and is reserved for the transmission of event-triggered/spontaneous messages. The sender in a dynamic window often needs to compete for bus access under a similar MAC mechanism as CAN protocol. As a result of the smart combination, FlexRay is theoretically an ideal fit for communication, especially in chassis domain, where time-critical messages are heavily mixed with event-triggered messages in transmission.

Another advantage of FlexRay in transmission is its high payload and low overhead. As can be calculated out from the FlexRay frame structure [55] in Fig. 4, the maximum payload of a FlexRay frame can reach up to 254 bytes and the corresponding frame length will be 262 bytes. According to (1), the maximum protocol efficiency of FlexRay is 96.95%.

However, it needs to be noticed that although FlexRay protocol has such high efficiency, the bandwidth cannot actually be fully exploited, mostly due to the unused space in the static segment and the unpredictable dynamic wastes. In order to cope with this deficiency and increase QoS, different approaches have been introduced. For instance, the idea of slot multiplexing in [56] can help better utilize the dynamic segment more efficiently. The unused static slots could be reduced by applying cost functions as described in [57]. Research in [58] reveals that the static segment could also be optimized in compliance with AUTOSAR specification. Moreover, the static slot can even be further exploited by pilfering the unused part for dynamic messages transmission, as described in the holistic method (HOSA) in [59]. By assigning the longest static message into the dynamic message, the wasted static segment in other different cycles can be reduced significantly [60]. In addition to the above mentioned methods, which mostly focused

on how to reduce the wasted bandwidth for a given static slot length, some experts have also opened a field by introducing the concept of 'FlexRay Switch', which uses slot multiplexing and branch parallelism to transmit different messages in the same time slot [61], [62], albeit subjected to the topology of the network.

Unlike the previously discussed LIN or CAN, FlexRay has much greater flexibility in topologies. As per [63], FlexRay supports various network structures ranging from point-to-point to different star connections, from linear passive bus to hybrid topology, even the connection types can vary between the two channels. This flexibility brings great convenience to EEA (Electrical Electronic Architecture) design in vehicles, but the cost and signal inconsistency problems coming with it should never be overlooked.

C. FlexRay Fault-Tolerance Capability

FlexRay possesses a bunch of distinctive features that help enhance its fault resistance capabilities. The most prominent feature is that it has two independent channels. The two channels are not only separated physically by different hardware paths (such as communication lines and bus drivers), but also carry out signal sampling, coding, decoding, and redundancy check, respectively [55].

Unlike other protocols, FlexRay has two CRCs (as shown in Fig. 4): one is the header CRC, the other is the trailer CRC. The header CRC is not calculated at every transmission, but configured and stored into the communication controller beforehand. Therefore, a corrupted header could hardly have a valid CRC. It has been further pointed out in [64] that FlexRay header CRC also provides protection to the length field, which may be overlooked by many other network protocols. The trailer CRC, on the contrary, is dynamically calculated, and well protects data integrity of all frame data including the CRC field. Moreover, the initialization vectors of the trailer CRC are different between the two channels, so as to prevent misconnection and increase fault-tolerant capabilities. The minimum HD of trailer CRC is 6 for a payload up to 248 bytes, but HD could also be reduced to 4 if the payload is greater than 248 bytes [55]. However, a FlexRay message with the latter payload is rarely seen in in-vehicle networks.

Inevitably, FlexRay also has some deficiencies in fault tolerant. For instance, FlexRay does not support fault notification/acknowledgement mechanism, which means the receiver will just discard the faulty message without notifying the sender. Since no retransmission is provided, if a static message fails to be delivered successfully in one slot, the sender has to wait till the next cycle (or the reserved window in the same cycle if well designed) for the next attempt.

To guarantee an acceptable QoS and reliable transmission, MILP (Mixed Integer Linear Program) has been adopted. It takes the linear deadline constraints of FlexRay messages into consideration, and explores possible optimizations of the existing schedule table, then utilize the spared static slots to add acknowledgement and retransmission mechanisms for faulty messages in the application level [65]. In addition, an approach to detect the transmission errors by comparing the extracted metadata has also been introduced, although at the expense of increased message overhead and delayed promptness [66]. Moreover, a heuristic distributed coordinator method is presented in [67], which can reconfigure the network, avoid network restart, and increase fault-tolerance, though it can only detect 80% individual errors. Some middleware technologies can also help increase QoS of FlexRay network. For instance, real-time middleware Data Distribution Service (DDS) [68] can be applied on top of FlexRay networks to provided guaranteed arrival of data at specific time.

Despite the inherent defects, the existing mechanisms, such as 32-bit CRC, bus guardian, mixed media access control and two independent channels, have already made FlexRay reliable enough for current safety-critical automotive applications [13].

V. Automotive Ethernet Network

With the increasing implementation of ADAS and multimedia functions in newer vehicles, broader vehicle network bandwidth is strongly demanded. Ethernet is a very promising candidate for the next generation in-vehicle network beyond CAN and FlexRay. It has acquired increasing attention from automotive industry in recent years [69]. As predicted in [70], Ethernet would have a penetration into new vehicles up to 40% in 2020.

A. Automotive Ethernet Cost Analysis

Ethernet as an emerging automotive network has unique advantages of sharing cost with other big industries such as IT (Information Technology) and Telecommunication, since high speed Ethernet at Gigabit/s level has already been extensively used in these industries. But Gigabit Ethernet is not suitable for automotive industry presently, due to the expensive shielded cable and high requirements of the internal processing units [71], [72]. This may partly explain why Ethernet was mostly used, at a much lower speed than Gigabit/s scale, only in applications such as ECU flashing rather than cameras or many other advanced safety systems in vehicles. Apparently cost was a key factor that had slowed Ethernet's penetration into the automotive market in the past.

Nowadays, the cost of Ethernet in vehicles has been reduced quite significantly since BroadR-Reach has been introduced. BroadR-Reach is an automotive Ethernet PHY (Physical Layer) technology developed by Broadcom and later on standardized by OPEN Alliance SIG consortium [73]. It supports multiaccess full-duplex transmission at 100 Mbit/s on a pair of unshielded twisted cables and is compatible with Media Independent Interface (MII) MAC. Therefore, it can be seamlessly integrated into the existing Ethernet networks, as shown in Fig. 5. Consequently, automotive Ethernet could possibly take advantages of the existing Ethernet infrastructures easily without much additional cost. Prior to the arrival of BroadR-Reach technology, the cost of a 10-meter-long fast in-vehicle Ethernet (100 Mbit/s) network excluding MCUs might be about 10 US dollars, but at present such a network may only cost 4~6 US dollars.

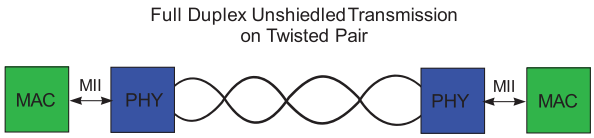


Fig. 5. BroadR-Reach PHY.

In the past camera and infotainment data were mostly transmitted through LVDS cables, but according to the prediction in [6], OEMs can save up to 80% of connectivity cost and 30% of cable weight by replacing the expensive and clumsy shielded LVDS lines with UTP Ethernet cables.

B. Automotive Ethernet Transmission Capability

In reference to OSI model, on-board single-frame Ethernet communication just requires layer one, two, and seven. Compared to other major in-vehicle networks, Ethernet has very high payload and protocol efficiency. Fig. 6 shows an IEEE 802.3 standard Ethernet packet format (the minimum frame size should be no less than 64 bytes), which clearly indicates that the maximum payload of an Ethernet packet is 1500 bytes with the packet length of 1538 bytes. In reference to (1), the maximum protocol efficiency of Ethernet equals 97.53%.

Earlier version of Ethernet resolves collision through CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism. When a station detects a collision in transmission, it will notify all other transmitting stations by transmitting jam sequence. After that the colliding stations will terminate the on-going transmission and retry accessing the network after a randomly distributed time interval. This mechanism is simple to implement, but cannot always guarantee packet deadlines with an increasing number of network stations and rising data load.

In modern in-vehicle Ethernet networks, collision problem is avoided by segmentation, where different stations are interconnected by high speed Ethernet switches. In fact, all Ethernet networks today are constructed in point-to-point topologies, where a collision domain will have only two nodes, and they communicate in full-duplex manner. In this case a station only communicates with the switch in the same collision domain, and never talks with other stations directly.

Currently BroadR-Reach technology is the de facto automotive industry standard for Ethernet PHYs. However, as pointed out in [74], 100 Mbit/s Ethernet is still not enough to transmit videos because of compression/decompression delays and bandwidth constraints (admittedly, this also depends on the quality of the video that needs to be transmitted). To tackle the bandwidth constraint, industries have already started effort to standardize IEEE 802.3bp as the next generation of automotive Ethernet PHY to realize Gigabit/s Ethernet transmission on RTPGE (Reduced Twisted Pair Gigabit Ethernet) [14], [75].

The mainstream trend of today's in-vehicle Ethernet, in addition to increasing the bandwidth and decreasing the cost, is to make it suitable for transmitting time-critical messages. This is also very critical to the success of the upcoming autonomous driving vehicles. As a result, several competent Ethernet high level protocols have been proposed, among which two most

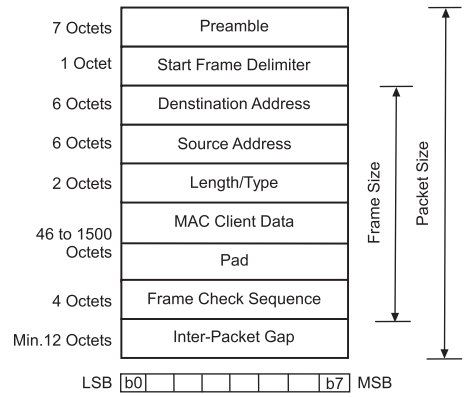


Fig. 6. IEEE802.3 Ethernet packet format.

prominent ones are IEEE Audio Video Bridge (AVB) [76], [77] and TTEthernet [78].

Initially as a standard to facilitate synchronized audio/video stream transmission through Ethernet networks, AVB has later on been found helpful to transmit time-critical signals in automotive networks. IEEE AVB task group has defined timing and synchronization [76], stream reservation [79], forwarding and queuing enhancement [80] for audio/video bridging systems [77]. The main idea of AVB is to use precisely synchronized global time (less than 1 μs error in maximum 7 hops, typically within ±300 ns [81]) to coordinate the transmission and reception of packets in the network. Network resources can be reserved along the packet path through declaration and registration mechanisms, so that the time sensitive stream will always have guaranteed transmission latency (2 ms for Class A traffic and 50 ms for Class B traffic). By implementing a dedicated forwarding and queuing mechanism, the registered data can be handled swiftly. To meet the required QoS, reserved traffic may be shaped, mapped and remapped in the switches.

Unlike AVB where QoS is maintained mainly by resource reservation and data prioritization, TTEthernet regulates data transmission and reception according to a preset table with global time synchronization. TTEthernet network guarantees determinism, but it only supports offline configuration. There are three different types of traffic defined in TTEthernet: Time Triggered (TT), Rate Constrained (RC) and Best Effort (BE). TT traffic has the highest priority and is preallocated to particular time slots, so its latency and jitter are quite small (much similar to FlexRay). On the contrary, RC and BE traffics are more like event-triggered types. RC traffic (similar to ARINC 664, Part 7) has a guaranteed maximum latency under certain bandwidth, which allows the data to be routed by a switch within a limited time, though it may be queued at buffer when multiple transmission requests appear simultaneously [82]. However, BE data can only be transmitted in the lowest priority, and has no guarantee of QoS at all. This 'incompetent' transmission pattern instead makes TTEthernet compatible with traditional LAN (Local Area Network) without protocol translation [83].

Although AVB and TTEthernet each has some unique capabilities in transmitting data in a timely manner, there are still ways to further enhance QoS of TTEthernet. For instance, a

novel offline configured traffic class AVB_ST has been introduced in [81], [84], [85], which can successfully reduce AVB's latency and jitter to a smaller extent. An improved worst case model in [86] could help reach tighter latency boundaries than the traditional worst case analysis in Avionics Full Duplex Switched Ethernet (AFDX) network. It is also applicable to TTEthernet networks. To tackle the rigid offline configuration problem of TTEthernet, a server-based scheduling algorithm is elaborated in [87], which provides online admission control and dynamic QoS management, and can be used in real-time applications as well.

C. Automotive Ethernet Fault-Tolerance Capability

Ethernet's capability to resist errors is related to multiple factors such as transmission media, payload, transmission mode, etc. For instance, using optical cable could significantly reduce BER than using unshielded electrical cables. The 32-bit CRC only has HD of 4 if the protected bit length is from 2975 to 91607, but HD could be raised to 5 if the protected bit length is 2974 or less [88]. MAC (CSMA/CD mechanism) only responds to collisions in half-duplex mode, but ignores them in full-duplex mode [75].

Nevertheless, there are still many efforts that could advance Ethernet's fault-tolerance capabilities. For example, researchers in [89] have contributed a seamless redundancy protocol that can increase fault tolerance in AVB stream reservation. The pros and cons of different schemes in integrating TTEthernet traffics has been well analyzed in [90], which can be used as a guidance for future improvement. PROFIsafe presented in [91] is worthy of consideration as well; it helps enhance error detection by introducing additional coding, sequence number, and acknowledgement mechanisms, although at the cost of increased processing time and energy consumption. As per [88], the existing CRC sequence of Ethernet may not be optimal. A better sequence has been proposed accordingly, which could raise HD to 6 with a payload of no more than1500 bytes. Furthermore, Bubbling Idiot problems can also be well handled by introducing "network fuse" as described in [92]. It works similar as the fuse in power circuit, and can cut off network channels connected to the failed nodes in order to protect the rest part of the network.

Middleware technology is useful in increasing QoS for Ethernet network as well. As pointed out in [93], middleware can also enhance the performance of the lower level protocols by many ways, such as adding extra CRCs if the Hamming Distance brought by the protocol CRC is not adequate. In addition, the middleware extension proposed in [94] could secure internet protocol based Ethernet communication in vehicles.

Admittedly, some concerns are not negligible, especially for AVB. For example, how to guarantee the authenticity in the declaration and registration process? How to dynamically manage the intricacy in Ethernet switches if the network grows very complicated [95]? However, both AVB and TTEthernet have been proven competent in multiple verifications for automotive 100M bit/s cases [82], [96]. Nowadays, these two protocols are both deemed as very promising contenders for the future in-vehicle Ethernet network standard, although some people tend to favor AVB more [14], [16].

A selected comparison between AVB and TTEthernet is shown in Table I.

TABLE I
SELECTED COMPARISON BETWEEN AVB AND TTETHERNET

	AVB	TTEthernet
Configuration	Online	Offline
Preemption	Yes	No
Jitter	High	Low
Tolerance	High	Low
BroadR-Reach	Compatible	Incompatible
Network Utilization	High	Low
Fault Tolerant	(Rapid) Spanning Tree or Shortest Path Bridging	Dual Redundancy
ADAS	Support	Support

VI. MOST NETWORK

Evolved from Domestic Digital Bus (D2B), MOST is a high speed network optimized for in-vehicle multimedia and infotainment data transmission. Developed by MOST Corporation, MOST network has advanced from MOST25 (Optical) to MOST50 (Electrical/Optic) and to the latest MOST150 (Electrical based on coaxial cable/Optical), and is reliable for the transmission of both synchronous and asynchronous data.

Over the years, MOST networks are under the growing influence of consumer electronic devices. The trend now is less number of ECUs in a MOST network, but ECU complexity and network bandwidth are increasing dramatically [97].

A. MOST Network Cost Analysis

Cost is a very crucial factor for MOST networks. Since its first introduction into automotive, MOST has been adopted by a rising number of vehicle models in the following years [98]. However, history has also witnessed some vehicle platforms abandoning MOST in their later models, simply due to the unacceptable high cost as compared to other in-vehicle networks.

The major cost of a MOST physical layer is not the POF (polymer optical fibers) cables, but the connectors and transceivers [99]. The primary reason is that the optical connectors have to be shielded and placed in separate cases, plus the optical transmitter and receiver often need to be made in two separate packages. Although MOST150 (MOST network with a bandwidth of 150 Mbit/s) supports electrical physical layer on coaxial cable, which is much cheaper than POF, a simplest MOST150 network may still cost around 10 US dollars on the physical components.

Along the years of development, many people have tried different methods to reduce the cost. For instance, MOST50 INIC (Intelligent Network Interface Controller) is capable of transmitting data through UTP instead of the expensive optical fibers (MOST150 on UTP has not been implemented in series production vehicles yet). It is also pointed out in [100]

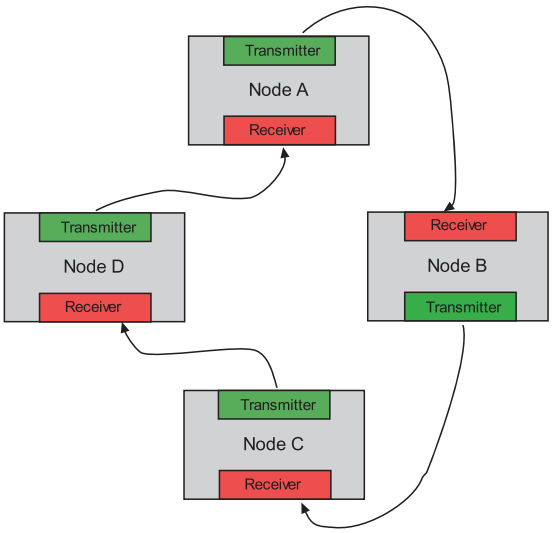


Fig. 7. Example of MOST ring topology.

that automakers could upgrade to MOST150 directly from MOST25 without changing their existing physical layers, and the cost may even be lowered if transmitter and receiver can be integrated in one SMD (Surface-Mounted Device) package. Meanwhile, some economical alternative optical-electrical transmission technologies, such as 'Optical Physical Bus Layer with Laser Diodes and Polymer Cladded Silica (PCS) Fibers' and 'Electrical Physical Bus Layer at 50 Mbit/s', are presently under rapid development [98].

Though the latest MOST150 has quite comparable unit node cost to MOST25 with a much higher bandwidth [97], MOST network as a whole is still very pricey among the popular in-vehicle networks.

B. MOST Transmission Capability

Different from the aforementioned networks, MOST involves all seven layers of OSI model for on-board communications [20]. An exclusive feature of MOST network is its unidirectional logic ring transmission pattern, which is often realized in a physical ring structure, but could also be implemented in a star topology. Unlike many other networks where the transmitter and receiver are integrated on one die and accessing the same physical cable, a MOST node has the transmitter (normally a light-emitting diode with 650 nm emission wavelength) and the receiver (normally a Silicon-PIN photodiode) in two separate components. An optical cable connecting them sequentially through different nodes forms a MOST network, as shown in Fig. 7.

MOST stands out from many in-vehicle communication networks because of its much higher bandwidth and versatility in transmitting different types of data. In the past years, MOST technology is constantly evolving to meet the increasing demands for transmission speed and data types. Generally, MOST supports the transmission of streaming data, packet data and control data at a baud rate from (approximately) 25 Mbit/s to 150 Mbit/s. The frame structures from MOST25 to MOST150 are shown in Fig. 8. According to (1), MOST150 has a maximum protocol efficiency of 96.88%, with the corresponding payload size and frame length of 372 bytes and 384 bytes, respectively.

Among the three MOST versions, MOST150 is the most promising one to be widely adopted in the near future by automotive industry due to many reasons. For instance, it has newly defined isochronous stream data transmission, which supports bandwidth reservation for three isochronous types of data (A/V packetized isochronous streaming, discrete frame isochronous streaming, and QoS isochronous mode). It can also be used to transmit audio/video streams that are not even synchronized to MOST time base [98], [101]. MOST150 also supports MAC addressing for packet data transmission, which could increase its compatibility with the popular Ethernet communication. Furthermore, it also has the maximum nominal bandwidth for control data, which would be quite suitable in transmitting large event-oriented packages. Though in reality not all bandwidth is available, owing to hardware and particular application limitations.

A comparison of some key parameters among different MOST types is provided in Table II.

C. MOST Fault-Tolerance Capability

Because of its high throughput and determinism, MOST150 is deemed by some experts as a perfect fit for ADAS [101], [102]. Firstly, the optical cables are immune to electromagnetic interference, and its communication error rate at the interface is lower than 10^{-9} [98]. Secondly, some other features, such as CRC and the ability to create redundant interconnecting rings [102], are also helpful in increasing its resistance to errors.

Unfortunately, MOST network is not immune to all possible errors, and still has some critical disadvantages in handling faults. For instance, due to its ring transmission structure, a defective MOST station may lead to total shutdown of the whole network, unless backup channels are present. Malicious timing frames is possible to disrupt MOST synchronization, while faulty channel requests may result in jamming the bus [103]. Since optical fiber only has very limited temperature adaptability, this may rule out the possibility of deploying MOST cables outside passenger compartment of vehicles. To maintain MOST operating at acceptable QoS, possible measures like AGF (All Glass Fiber) wire harness [101] and redundant MOST path design [104] may be adopted by the industry in the near future. Other possible enhancements of MOST network include strengthening its interoperability with Ethernet AVB [105] in order to build an efficient cross-domain communication system, and further boosting its bandwidth to transmit uncompressed video streams with higher resolution [106].

VII. Automotive Gateway and Vehicle-Wide Network Topology

Since a modern in-vehicle communication system is nearly always a combination of various subnetworks running with different communication protocols, automotive gateways as the interfaces between different subnetworks are vital to the overall in-vehicle communication network, and should never be neglected.

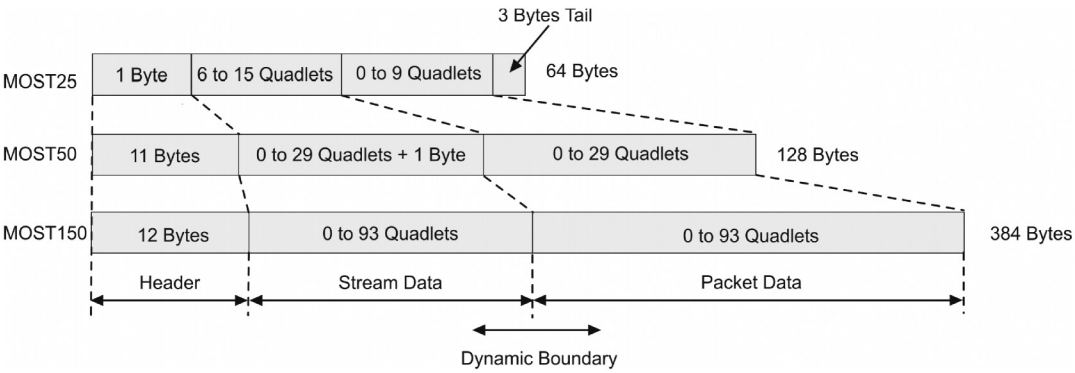


Fig. 8. Basic structure of MOST frames.

TABLE II
FRAME PARAMETERS OF MOST25, MOST50 AND MOST150 [100]

	MOST25	MOST50	MOST150
Frame size(bits)	512	1024	3072
Sample rate(kHz)	44.1	48	48
Streaming data			
Minimum(bytes)	24	0	0
Maximum(bytes)	60	117	372
Minimum bandwidth (Mbit/s)	8.467	0.384	0
Maximum bandwidth (Mbit/s)	21.168	44.928	142.848
Packet data			
Minimum(bytes)	0	0	0
Maximum(bytes)	36	116	372
Minimum bandwidth (Mbit/s)	0	0	0
Maximum bandwidth (Mbit/s)	10.841	44.544	142.848
Control data			
Bytes per frame	2	4	4
Minimum number of frames	16	6	6
Maximum number of frames	16	9	18
Minimum data bytes	19	7	8
Maximum data bytes	19	19	53
Minimum gross bandwidth (Kbit/s)	405.84	448	512
Maximum gross bandwidth (Kbit/s)	405.84	810.62	1130

There are generally three possible functionalities of an automotive gateway in a communication system. Firstly, it may work as a protocol bridge to facilitate data transmission across different subnetworks. This is also the most orthodox role of a gateway. Secondly, it can be used to "expand" network bandwidth, where the gateway is connected to other subnetworks of the same protocol so as to avoid overloading one network section. Thirdly, a gateway can work as a firewall, where it behaves as a guard to fend off the unauthorized external accessing attempts and minimize the undesired disturbances.

There are two classifications for gateways. If based on routing mechanisms gateways can be categorized as either message routing or signal routing. If based on the overall function of the ECUs, gateways can be classified as either independent or integrated.

A message routing gateway normally routes the ingress messages to the designated subnetwork(s) according to the routing table, sometimes even without changing the ID or the transmission period of the incoming message (e.g., route to a network of the same protocol but with different baud rate). In reference to the OSI model, only functions up to the network layer are needed to accomplish message routing. Conversely, a signal routing gateway needs to unpack the ingress messages, reconstruct new messages, and send them to the designated subnetwork(s). Normally signal routing gateways are more computationally demanding than the massage routing ones, and may need software implemented higher than network layer in regard to the OSI model. Gateways between different protocols (e.g. between CAN and FlexRay, or between CAN and Ethernet) are definitely of signal routing type.

On the other hand, an independent gateway is the one that only works for routing and does not have any other application functions (normally except network management and diagnostics). An integrated gateway does not only route messages, but also behaves partly as a normal ECU with other functionalities, such as body control or illustration panel control.

In in-vehicle network designs, the choice between independent and integrated gateways mostly depends on the cost and computational capability of the ECUs. Integrated gateways are cheaper, but require more computational power, as they also need to accomplish non-routing tasks at the same time. Independent gateways may cause additional hardware cost such as new ECUs and wires, but could bring in great flexibility and convenience in system design, component test, maintenance and even packaging.

When it comes to designing an automotive network gateway for real-world applications, the process becomes more complicated, and could vary from case to case. In a highly distributed in-vehicle network, how to address the challenges of rising network complexity with large amount of interdomain communication, stringent timing requirements, and increasing bandwidth demand has become a hot topic in automotive gateway research nowadays [107]. Furthermore, software architecture of the gateway is very critical, too. As gateways can be quite flexible in automotive, its software should also be very easy to implement and meet the quality requirements such as reliability, maintainability, reusability and portability for future development.

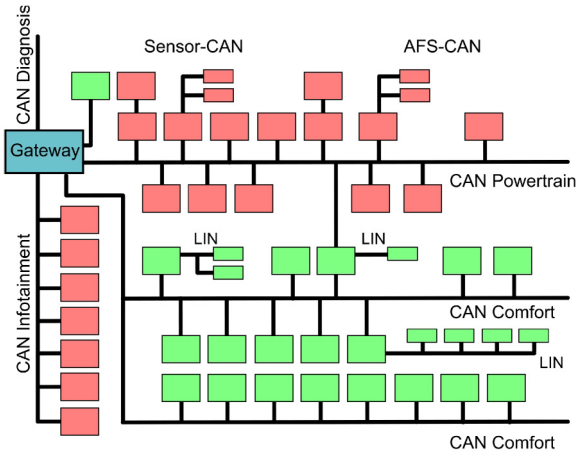


Fig. 9. Centralized gateway design in Volkswagen Passat network topology.

A popularly adopted in-vehicle network topology in the past was a centralized gateway with different subnetworks all connected to it, such as Volkswagen Passat network topology in Fig. 9. BMW 7 series and Audi also followed the similar centralized gateway design in [12], [13]. However, such gateway design strategy may not fit today's needs as more high-bandwidth and low-latency data are exchanged between subsystems. Instead, contemporary automotive gateways tend to be more compact. The functions of the centralized gateway may be distributed into multiple nodes in order to prevent overloading a single node. It can also avoid the failure of the whole network caused solely by the malfunction in the central gateway.

To demonstrate how different types of networks are typically used and how they are integrated together through gateways, an exemplary high-end vehicle network topology is presented in Fig. 10.

In the presented architecture, Ethernet is only used as a high bandwidth communication channel between the external tester and the vehicle connectivity module, typically to reduce the time of ECU flashing and EOL (End Of Line) configuration. FlexRay, though not as an X-by-Wire carrier in this case, is used as the network backbone, owing to its high enough bandwidth and outstanding determinism. CAN is irreplaceable in many intra-domain communications, because it has already been proven very reliable and easy to implement in many previous projects. In spite of very low baud rate, LIN network is still widely adopted at peripheral applications, thanks to its simplicity and low cost. MOST remains the common choice for infotainment system, which usually requires the highest bandwidth in the network.

One prominent feature in the topology is the increasing number of wireless modules. These modules may communicate through various ways, such as Wi-Fi, Bluetooth, Radio Frequency, or Telecom Networks, depending on specific applications. This signifies an important trend that today's customers are willing to see more connectivity between their personal electronic devices and the vehicles. It also implies that infotainment data will possibly gain more access into in-vehicle networks in the future.

Another noticeable feature is the domain specific network structure. The ECUs that exchange information most frequently are grouped into the same domain and separated from other sections of the network by gateways. Gateways are normally the domain masters and protect the downstream subnetworks from undesired disturbances. Moreover, such domain specific composition can reduce bus load and provide relative independence to the subnetworks. This is quite helpful in increasing subsystem portability and restraining development cost in future projects.

VIII. Security Challenges and Features of In-Vehicle Networks

In addition to the previously discussed aspects, security is another rapidly emerging challenge to the in-vehicle networks. Security problem, in the context of in-vehicle networks, often refers to the risky situations that communication data may be eavesdropped, spoofed, discarded, modified, flooded, stolen, or replayed by malicious attackers. In the time that vehicles are evolving towards autonomous and cooperative driving, security has become ever more critical in the design of in-vehicle networks.

A. Security Threats to In-Vehicle Networks

Security problem was not a primary concern when the in-vehicle network protocols were invented. Thus, many security features were inherently missing. For instance, CAN lacked necessary protection to ensure signal availability, confidentiality, and authenticity [108]. FlexRay, though capable of maintaining correct operation in the presence of errors, could not fend off well-formed malicious error messages [109]. Nevertheless, these disadvantages did not pose imminent security threats in the past, as vehicles were rarely connected to the outside world and the old-fashioned security attacks often required physical access to the in-vehicle networks.

However, modern vehicles are rapidly becoming more connected through various means for many advanced applications. For instance, vehicles may be connected through DSRC (Dedicated Short-Range Communications) for VANETs (Vehicular Ad-Hoc Networks) features, through Wi-Fi/Bluetooth for on-board entertainment, and through cellular network for telematics services. Although these connections have made the vehicles more intelligent and comfortable, they also expose the in-vehicle networks heavily to the external adversaries. For instance, CAN communication could be potentially tampered through smart phone malware remotely via cellular network [108]. Software virus is possible to propagate to in-vehicle components through the infected entertainment media, such as CDs (Compact Disc) or Bluetooth players [110]. Furthermore, it is also possible to break into in-vehicle network by attacking the bad management of ECU keys in OEMs' storage centers.

In addition, the threats from direct access still exists, as adversaries may also break into the communication line physically and launch attacks directly against the weakness of network components. Typical attacks of this kind may include

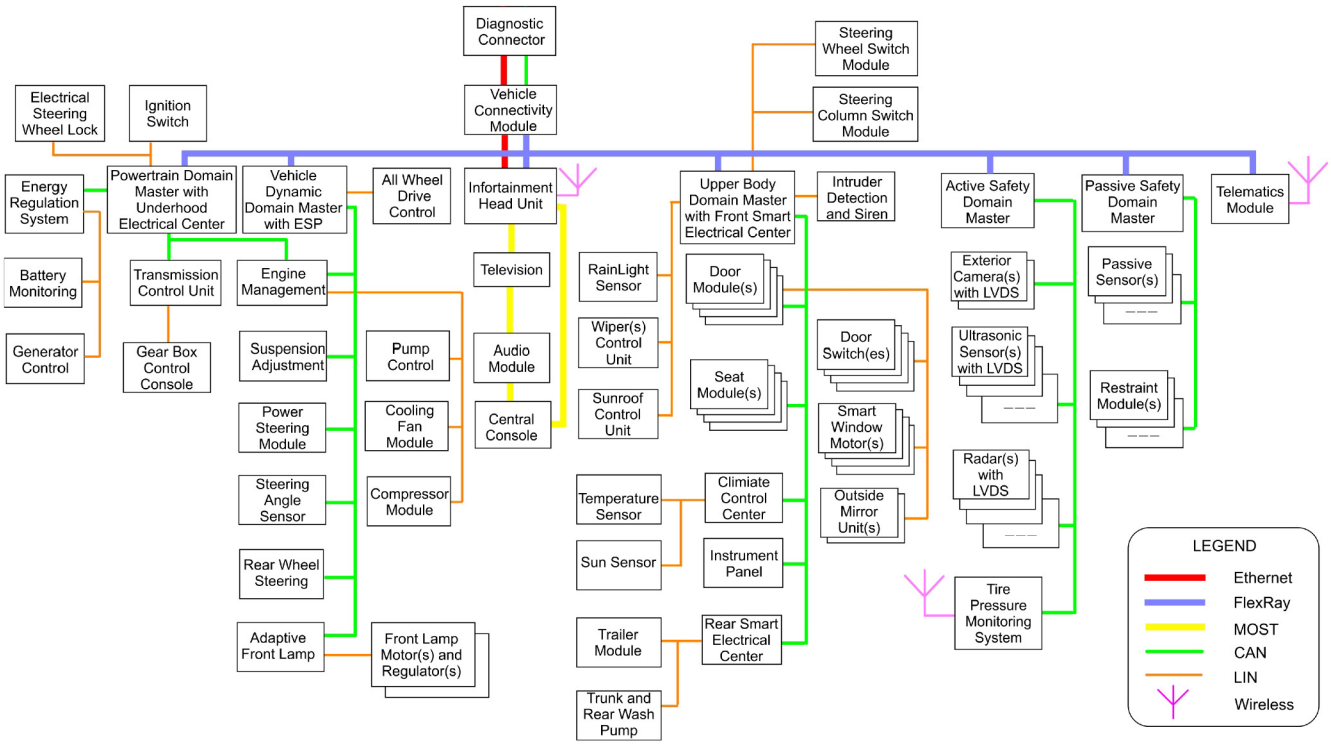


Fig. 10. Exemplary topology of in-vehicle network topology.

disassembling the executable code and injecting malicious code to the runtime environment.

Security breaches of in-vehicle networks may not only cause severe consequences to the vehicle users, but to other road traffic participants as well. For instance, security breach may cause privacy leakage of the vehicle users. The targeted private data may include vehicle diagnostic stream, cabinet conversation, camera record, driving pattern, and vehicle positions [109]–[112]. Typical attacks of such kind is conducted through unauthorized eavesdropping. Secondly, security breach could lead to direct monetary loss of the vehicle owners or the OEMs. In such attacks, adversaries often intentionally modify or replay the desired in-vehicle data to achieve illegal gains, such as vehicle theft or odometer fraud. The third level of security breach may cause safety threat to the vehicle users. This kind of attacks often involves malicious modification or forgery of the safety critical in-vehicle data, such as tire pressure, vehicle speed, engine torque request and brake command [108]. This may lead to involuntary driving maneuver or even traffic accidents. Considering the advent of autonomous driving, such hazard is vital and deserves more attention from the research community. Fourthly, in-vehicle network security breach can incur safety threats to other road participants, and even paralyze the whole traffic system. Since vehicles are to be interconnected in a massive network, such as VANETs, signal trustworthiness are extremely critical to all the vehicles in the coordinate traffic systems [113]. However, this trustworthiness could be ruined if the in-vehicle network security is compromised. For instance, the tampered in-vehicle networks may originate false data, which could cause great danger to other vehicles, if the false data have propagated to the outside of the vehicle and picked up by others as 'trustworthy'.

A brief summary of different security attacking types, along with typical targets, possible consequences, and relative severity, is provided in Table III.

B. *Security Features to Protect In-Vehicle Networks*

Security features are indispensable for all of today's in-vehicle networks. The efforts to secure in-vehicle networks are mainly made from three perspectives: limiting physical access, strengthening the weakness of the protocols, and better managing key storage and transportation.

Limiting physical access is the most direct way to protect in-vehicle networks. It has long been adopted by the automotive industry. A common approach to do so is deploying a central gateway behind the OBD-II connector, which can isolate the in-vehicle networks from external attacks (as mentioned in Section VII). Another approach is restricting the connectivity of particular network nodes, such as the LIN slaves in outside mirrors. This could protect a locked vehicle from being hacked through a snapped outside mirror [114]. It is also worth pointing out that Ethernet has the highest capability to prevent eavesdropping than other bus-connected in-vehicle networks, thanks to its point-to-point connection fashion.

However, simply limiting physical access is not enough, as the online data may still be intercepted through various channels. Therefore, most of the recent efforts are focused on how to prevent the exposed data from being interpreted or manipulated by the adversaries [115]. To achieve such goals, cryptography and authentication are the two most widely adopted methods. But in real-life applications, the suitability of a certain secure approach may vary from network to network.

TABLE III
SECURITY ATTACKS OF IN-VEHICLE NETWORKS

Attack Means	Typical Targets	Consequences	Relative Severity
Eavesdropping	In-Vehicle Conversation, Camera Record, Driving Pattern, Vehicle Position	Privacy Leakage	Low
Impersonation, Modification, Stream Replay	Remote Key Entry, Immobilization, DVD player, Odometer Readings	Direct Financial Loss	Low to Medium
Modification, Impersonation	Vehicle Speed, Radar Data, Steering Command, Brake Interference, Engine Torque Request	Involuntary Maneuver, Life Threat to the Vehicle Users	High
Flooding, Dropping, Modification, Impersonation	Vehicle Speed, Direction of Movement, Driver's Command, Collaborative Decisions in Intelligent Traffic Applications	Traffic Paralysis, Denial of Service, Life Threat to All Road Traffic Participants	High

Cryptographic solution is to encrypt the message so that only the authorized person with the correct decryption key could read it. AES (Advanced Encryption Standard) is a widely accepted approach, which supports both symmetrical and asymmetrical encryptions, and is considered cryptographically secure from today's perspective [116]. However, even the most commonly used AES algorithm, AES128, may have problems in applying to LIN and CAN networks, as their payloads are too small for a full-size AES algorithm. For instance, research in [108] has proposed a new method to encrypt CAN transmission with a combination of AES128 and Keyed-Hash Message Authentication Code, but only the truncated result is extracted owing to payload limitation. Nevertheless, CANFD and other major in-vehicle networks are suitable for AES encryption. For time-triggered networks such as FlexRay and TTEthernet, a zero latency encryption approach can be adopted [117], which integrates encryption functions into the TT messages without affecting their real-time nature. For the networks with centralized-gateway topology, the approach in [118] is applicable, in which the gateway performs as the super center to encrypt all the cross domain communications. In addition, some lightweight encryption mechanisms are proposed to lower the hardware requirement of communication system. For instance, ALE in [119] is a single-pass nonce-based online scheme that is much smaller and faster than many existing AES schemes. The hybrid cryptosystem in [120] has the minimum memory requirement among many contemporary ciphers by combining the confusion capable group operation and the S-box of PRESENT crypto engine.

On the other hand, authentication is the mechanism by which the network node can justify whether the message is coming from an authentic partner and untampered. There are various ways to realize authentication in in-vehicle networks. For instance, it can be achieved by membership management, where ECUs are assigned different memberships and only the designated members are able to read and write the messages correctly [121]. It can also be done by attaching message authentication code to every transmission, so that the receivers could use it to verify the authenticity of the incoming message [122]–[124]. Authentication methods are generally applicable to all major in-vehicle networks. For those with higher bandwidth, such as FlexRay, MOST, and Ethernet, higher authentication overhead is tolerable, thus more complicated authentication code and greater security performance can be expected. In order to safely distribute the security keys to the designated nodes, a lightweight authentication framework can be adopted [125]. Additionally, researchers in [115] have pointed out that VLAN (Virtual Local Area Network) technology, though primarily used in Ethernet, can similarly be used to add authentication for other networks in principle. For the TDMA based systems, it is also possible to deploy the mechanism in [126] to protect the protocols against attacks, which adopts time-delayed release of keys to authenticate the messages.

However, it should be noticed that apart from the payload and bandwidth constraints, the effectiveness of a certain encryption or authentication mechanism may also subjected to many other constraints, such as timing requirements and resources availability of the specific networks.

In addition to the aforementioned approaches, other methods are also helpful to secure in-vehicle networks. For instance, a novel hardware security module is designed and evaluated in [127], which can provide holistic protection of all relevant in-vehicle ECUs and their communications. Moreover, enhancing software bootloader can prevent the network against certain attacks, such as illegal ECU flashing [128]. Furthermore, the efforts to strengthen the safety of VANETs [129], [130] and OEM data centers are also beneficial to the safety of in-vehicle networks.

Based on the discussion above, a summary of some selected security features and their suitability to different in-vehicle networks is presented in Table IV.

IX. SUMMARY AND OUTLOOK

This article has reviewed five currently most popular in-vehicle communication networks. Analyses and comparisons are presented mainly from the perspectives of system cost, communication capacity and fault-tolerant capabilities. The main features of each network are summarized below.

LIN network has unparalleled cost advantages and engineering simplicity. These features make it remain popular in many low-speed and simple applications. After decades of development, CAN communication has become a well-accepted and reliable technology. However, standard CAN today can no longer meet either timing or bandwidth requirements for the popular safety systems such as ADAS. FlexRay has the highest determinism and fault-tolerance presently, therefore it is quite suitable for vehicle dynamics and safety controls. In practice,

TABLE IV
SELECTED SECURITY FEATURES AND THEIR SUITABILITY TO DIFFERENT IN-VEHICLE NETWORKS

Category	LIN	CAN	FlexRay	Ethernet	MOST	Comments
Physical Access Restriction	Slave Connectivity Restriction, Central Gateway Isolation	Central Gateway Isolation	Normally No Direct Exposure	Point-to-Point Connection, Isolation	Normally No Direct Exposure	Closed vehicle body and well-hidden network cable are the best barriers of physical access
Encryption	Central Gateway Encryption, ALE, Hybrid Cryptosystem	AES, Central Gateway Encryption. ALE, Hybrid Cryptosystem	AES, Zero Latency Encryption, Central Gateway Encryption, ALE, Hybrid Cryptosystem	AES, Zero Latency Encryption, ALE, Hybrid Cryptosystem	AES, Central Gateway Encryption, ALE, Hybrid Cryptosystem	• In reality encryption and authentication solutions are seldom used on LIN • Traditional CAN cannot use untruncated AES results, but CANFD is capable to do so • The suitability depends on the underlying network and the availability of resources • Many encryption and authentication methods used in VANETs are also applicable in principle
Authentication	Membership, Message Authentication Code	Membership, Message Authentication Code,	Membership, Message Authentication Code, time-delayed release of keys	Membership Message Authentication Code, VLAN, time-delayed release of keys	Membership, Message Authentication Code	
Other Measures	Adopting Hardware Security Module, Enhancing ECU Bootloader, Securing Inter-Vehicle Communications, Strengthening the Protection of OEM Data Center, etc.					Protect in-vehicle networks by fortifying the network nodes and ensuring the correctness of external data

TABLE V
SELECTED COMPARISONS OF IN-VEHICLE NETWORKS

Network	Relative System Cost	Typical Bandwidth (bit/s)	Max. Protocol Efficiency (%)	Relative Fault-Tolerance	MAC Mechanism	Typical Topology	Layers in OSI Model	Security Threats	Typical Applications in Vehicles
LIN	Low	11.2K or 19.6 K	51.6	Low	Polling	Linear Bus	1,2,7	Low	Battery Monitoring, Window Lifter Control, Steering Wheel Button Assembly, Temperature Sensors, Blower Control, Sunroof Module, Alternator Module
CAN	Low to Medium	125K or 500K	59.26	Low to Medium	CSMA/CA	Mostly Linear Bus	1,2,7	High	Engine Controller, Transmission Unit, Electrical Stability Control, Seat Module, Cluster Control, Upper Body Control, Climate Control, Seat Module, Smart Electrical Centers, Headlamp Assembly, Trailer Module, Standard OBD-II Interface
FlexRay	High	5M or 10M	96.95	High	TDMA	Linear Bus, Star, or Hybrid	1,2,7	Medium	Steering Angle Sensor, Safety Radars, All-Wheel Drive, Throttle Control, Dynamic Suspension Control, Supplementary Restrain System, Active Safety System, Network Backbones
Ethernet	Medium	100M	97.53	Medium to High	CSMA/CD	Point-to-Point	1,2,7	High	ECU Flash Interface, Cameras, Lidars, Safety Radars, Entertainment Unit, Wireless or Consumer Electronics Connector, Network Backbones,
MOST	Medium to High	25M, 50M or 150M	96.88	Medium	Time Division Multiplex/ CSMA	Ring	All Layers	Medium to High	Infotainment Head Unit, Central Console Display, Amplifier Control, Rear Seat Entertainment Unit, Audio Module, Navigation System

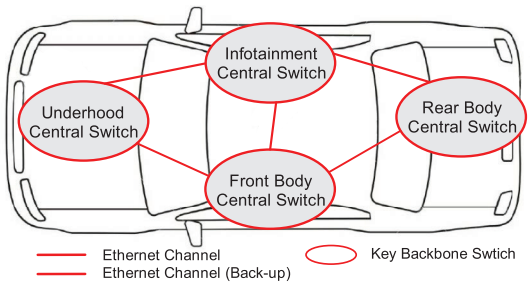
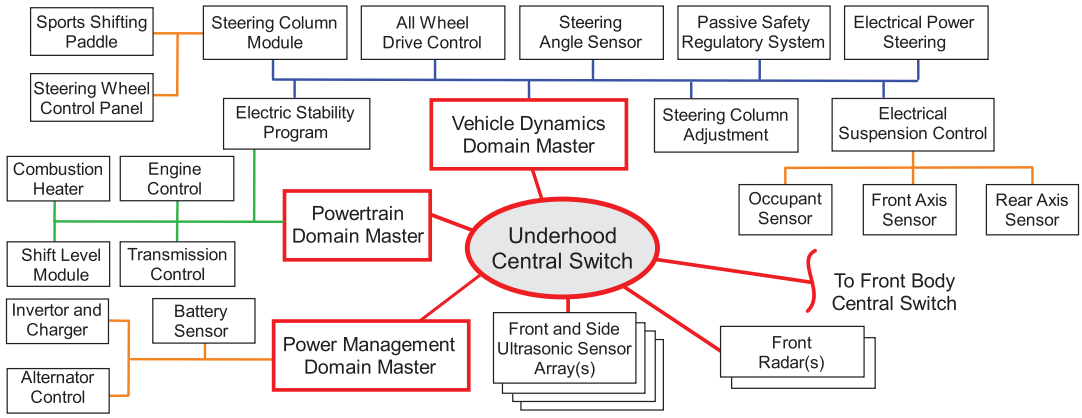
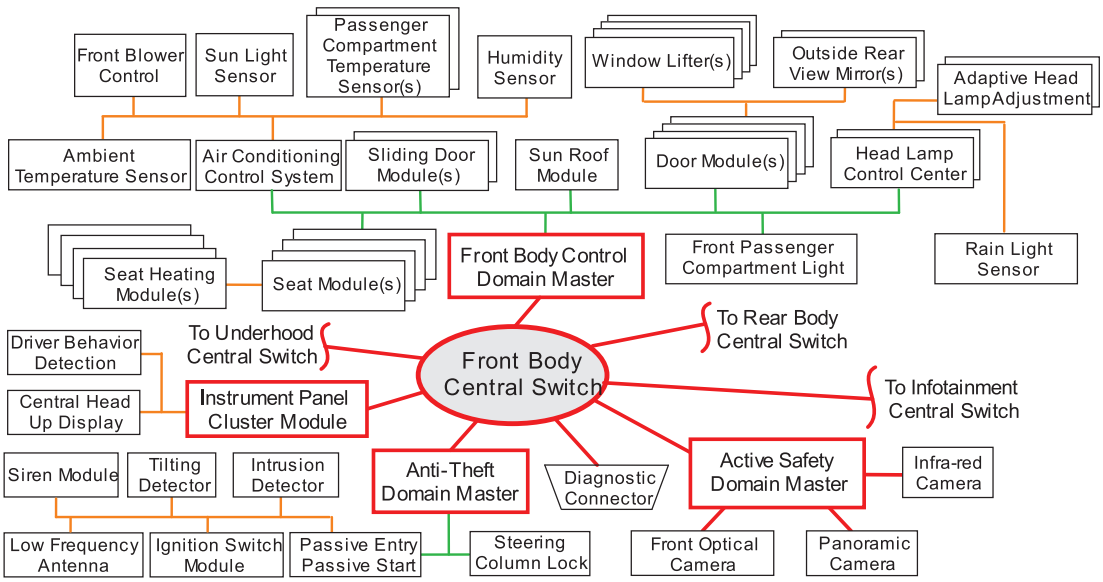


Fig. 11. Proposed abstract structure of next-generation in-vehicle network topology.

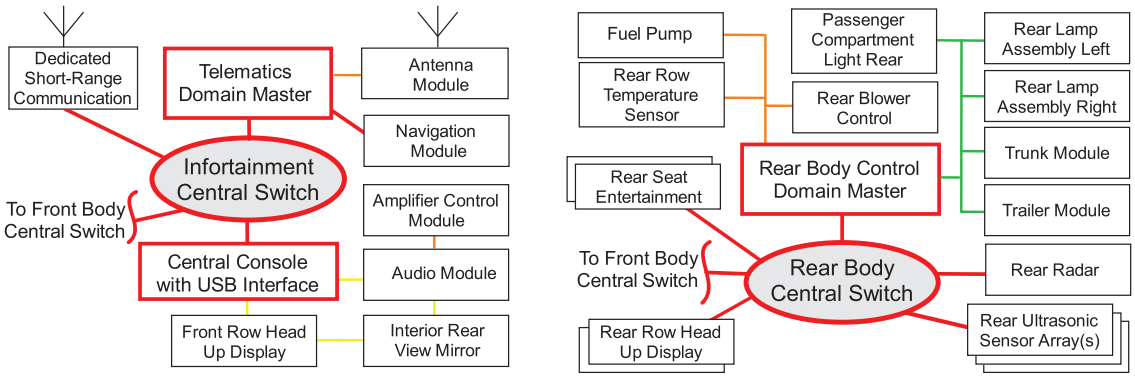
only a limited number of vehicle models have actually used FlexRay for X-by-Wire systems so far. Many others just take advantage of its wide bandwidth and high determinism, and use it solely as the communication backbone at the present. A FlexRay system is still relatively expensive and has high engineering complexity at the current stage, which may impede its fast expansion into many other fields. Ethernet is an emerging communication technique for in-vehicle communication networks, though it has already long been used in many other industries. With the advancement of low-level technology such as BroadR-Reach (as well as the upcoming RTPGE) and the



(a) Proposed network topology of underhood domain.



(b) Proposed network topology of frond body domain.



(c) Proposed network topology of infotainment domain and rear body domain.

Fig. 12. Proposed abstract structure of next-generation in-vehicle network topology in detail. (a) Proposed network topology of underhood domain. (b) Proposed network topology of frond body domain. (c) Proposed network topology of infotainment domain and rear body domain.

high-level protocols such as AVB and TTEthernet, automotive Ethernet network has shown significant reduction in cost and promising performance in deterministic transmission in recent years. It may gradually turn the whole in-vehicle network towards fully end-to-end Ethernet solution [14], [16]. Future developments may focus on how to combine the benefits of both AVB and TTEthernet [82], and transmit both types in the same network at an increased bandwidth, so as to accommodate the surging demand for high resolution cameras and upgraded multimedia systems [96]. Although being claimed in [101] as the best positioned network to integrate many other in-vehicle networks, MOST still requires much advancement in both transmission and fault-resistance capabilities. Currently, it has only been successfully deployed in infotainment and navigation systems on series production vehicles. The performance of the latest MOST150 network is still far below the theoretical limit of MOST technology. It is expected to have plenty of room for development in the future.

A summarized comparison of some selected features among LIN, CAN, FlexRay, Ethernet and MOST networks is given in Table V.

It is also highlighted in this paper that gateways are very important for an advanced in-vehicle communication system. They are not only bridging between the networks running on different protocols, but also playing critical role in coordinating data transmission among all the subnetworks and making the whole system run correctly. From the technical point of view, meeting signal latency requirements needs to be given the highest priority in a gateway design. The developers should guarantee that the worst-case signal latency is always within the boundary of functional requirements under all circumstances.

However, in real engineering applications, it is actually a comprehensive process to select an appropriate protocol, design a particular subnetwork, and integrate different subnetworks into an organized communication system. Apart from system cost, transmission capacity, and fault-tolerance capabilities, there are many other equally essential aspects which need careful contemplation, such as high level EEA definition, subsystem functional partitioning, layered software integration, wire harness design, network/power management strategy, even the convenience of aftersales maintenance.

With the movement towards autonomous and cooperative driving, communication security has quickly become a critical concern in the design of in-vehicle networks. This paper has also analyzed the importance of in-vehicle network security, and categorized the consequences of security breaches into four different levels based on the severity. It is pointed out that in addition to limiting the physical access, various cryptography and authentication solutions can also be used to protect in-vehicle networks. As more powerful controllers being introduced into the vehicles, security algorithms are expected to be more sophisticated to provide better protection for in-vehicle communications.

It is very likely that Ethernet will lead the advancement of the next-generation in-vehicle networks in the future. Its competitiveness comes from its high bandwidth, the low cost PHY techniques like BroadR-Reach, and the rapidly evolving deterministic Ethernet technologies such as AVB and TTEthernet. Based on the researches in this paper, an abstract topology of the next generation in-vehicle network is proposed in Fig. 11, and further expanded in detail in Fig. 12. It is believed the next-generation in-vehicle communication networks may have the following features:

1) Ethernet will become the backbone of the network to provide deterministic, high-bandwidth, and fault-tolerant connectivity among different subsystems. It will also have increased adoption in both safety-related and infotainment-related applications.
2) The development of ECUs would become more domain intensive (also called zone-oriented) to ensure better system independence and portability.
3) All existing major protocols will still be used based on various requirements on system cost, transmission capability, and fault-tolerance. But traditional CAN may give way to CANFD in some cases and MOST may see strong challenges from Ethernet.
4) More security features will be implemented in in-vehicle networks, in order to meet challenges brought by the intelligent systems, such as ADAS, autonomous, and cooperative driving systems.
5) In-vehicle network platforms will become more complex and comprehensive. Thus, OEMs may maintain less number of platforms, but would derive more variants from the platform superset to increase design flexibility and reduce cost.
6) Consumer electronics with different kinds of connections, such as USB and various wireless interfaces, would obtain more access into the wired in-vehicle networks. New propriety connector(s) may also be used in addition to the OBD-II connector.
7) Networks may be monitored and configured through a principal network master, which could also provide additional safety margins for the whole network.
8) The interfaces between different communication software components would become further standardized, and software interchangeability will be significantly developed.

ACKNOWLEDGMENT

The authors declare no competing financial interests with the respective sponsors.

REFERENCES

[1] K. Pretz, "Fewer wires, lighter cars," IEEE—The Institute, Piscataway, NJ, USA, Apr. 12, 2013 [Online]. Available: http://theinstitute.ieee.org/benefits/standards/fewer-wires-lighter-cars, accessed on Nov. 07, 2014.

[2] J. Chacko, "Electrical build issues in automotive product development," M.S. thesis, Syst. Design Manage. Program, Massachusetts Inst. Technol., Cambridge, MA, USA, 2007.

[3] T. R. Egel, "Wire harness simulation and analysis techniques," SAE International, Warrendale, PA, USA, Tech. Paper 2000-01-1293, 2000.

[4] H. Kimm and H. Ham, "Integrated fault tolerant system for automotive bus networks," in *Proc. IEEE 2nd Int. Conf. Comput. Eng. Appl.*, 2010, pp. 486–490.

[5] J. B. Anderson, *Digital Transmission Engineering*, 2nd ed. Hoboken, NJ, USA: Wiley, 2008.

[6] R. Boagey, "Ethernet: The fast track to the connected car," in *Automotive Megatrend Magazine*. Penarth, U.K.: Automotive World Ltd, 2014, pp. 36–38.

[7] A. Camek *et al.*, "An automotive side-view system based on Ethernet and IP," in *Proc. IEEE 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Fukuoka, Japan, 2012, pp. 238–243.

[8] *Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model*, ISO/IEC 7498-1, 1994.

[9] OSEK VDX Portal. *Welcome to OSEK VDX* [Online]. Available: http://www.osek-vdx.org/, accessed on Jul. 24, 2015.

[10] Mentor Graphics. (2014). *Volcano Network Architect (VNA)* [Online]. Available: http://www.mentor.com/products/vnd/communication-management/vna/, accessed on Nov. 08, 2014.

[11] AUTOSAR (AITomotive Open System ARchitecture). (2015). *AUTOSAR Specification Release 4.2* [Online]. Available: http://www.autosar.org/, accessed on Feb. 04, 2016.

[12] N. Navet and F. Simonot-Lion, *Automotive Embedded Systems Handbook*. Boca Raton, FL, USA: CRC Press, 2009.

[13] U. Keskin, "In-vehicle communication networks: A literature survey," Computer Science, Technische Universiteit Eindhoven (TU/e), Eindhoven, The Netherlands, Tech. Rep. 09-10, 2009.

[14] S. Tuohy *et al.*, "Intra-vehicle networks: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16. no. 2, pp. 534–545, Apr. 2015.

[15] S. C. Talbot and S. Ren, "Comparison of field bus systems CAN, TTCAN, flex ray and LIN in passenger vehicles," in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Montreal, Quebec, Canada, 2009, pp. 26–31.

[16] S. Tuohy *et al.*, "Next generation wired intra-vehicle networks, a review," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Gold Coast City, Australia, 2013, pp. 777–782.

[17] N. Navet and F. Simonot-Lion, "In-vehicle communication networks—A historical perspective and review," in *Industrial Communication Technology Handbook*, vol. 96, 2nd ed. Boca Raton, FL, USA: CRC Press, 2013.

[18] National Instruments. *FlexRay Automotive Communication Bus Overview*. (2009) [Online]. Available: http://sine.ni.com/np/app/main/p/ap/icomm/lang/en/pg/1/sn/n17:icomm,n21:11972/fmid/2924/, accessed on Nov. 09, 2014.

[19] *LIN Specification Package, Revision 2.2A*, LIN Standard, LIN Consortium, 2010.

[20] A. Diarra, "OSI layers in automotive networks," presented at the IEEE 802.1 Plenary Meeting, Orlando, FL, USA, 2013.

[21] C. Quigley *et al.*, "Design approaches for integrating CAN with emerging time-triggered protocols," *presented at IEEE Int. Conf. Commun.*, Istanbul, Turkey, 2006.

[22] P. Koopman, "Tutorial: Checksum and CRC data integrity techniques for aviation," Electr. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, May 2012 [Online]. Available: https://users.ece.cmu.edu/~koopman/pubs/KoopmanCRCWebinar9May2012.pdf, accessed on Feb. 03, 2016.

[23] T. C. Maxino and P. J. Koopman, "The effectiveness of check sums for embedded control networks," *IEEE Trans. Depend. Secure Comput.*, vol. 6, no. 1, pp. 59–72, Jan./Mar. 2009.

[24] G. Miller. (2013). *Automotive Communication Protocols: Preparing for the Future Embedded Systems Engineering* [Online]. Available: http://eecatalog.com/automotive/2013/03/13/automotive-communication-protocols-preparing-for-the-future/, accessed on Nov. 07, 2014.

[25] O. Pfeiffer. *Selecting a CAN Controllerv, Embedded Systems Academy* [Online]. Available: http://www.esacademy.com/en/library/technical-articles-and-documents/can-and-canopen/selecting-a-can-controller.html, accessed on Nov. 07, 2014.

[26] *Road Vehicles – Controller Area Network (CAN) – Part 2: High-Speed Medium Access Unit*, ISO 11898-2:2003.

[27] *Road vehicles – Controller area network (CAN) – Part 5: High-Speed Medium Access Unit With Low-Power Mode*, ISO 11898-5:2007.

[28] *Road vehicles – Controller area network (CAN) – Part 3: Low-Speed, Fault-Tolerant, Medium-Dependent Interface*, ISO 11898-3:2006.

[29] *Single Wire Can Network for Vehicle Applications, SAE International* 2411A (WIP), 2000.

[30] *CAN Specification, Version 2.0*, CAN Standard, Robert Bosch GmbH, Gerlingen, Germany, 1991.

[31] W. Lawrenz, Ed., *CAN System Engineering: From Theory to Practical Applications*, 2nd ed. New York, NY, USA: Springer, 2013.

[32] S. Corrigan, "Critical spacing of CAN bus connections," Appl. Rep. Texas Instrum., Dallas, TX, USA: Tech. Rep. SLLA279A, 2009.

[33] M. Di Natale *et al.*, *Understanding and Using the Controller Area Network Communication Protocol*. New York, NY, USA: Springer, 2012.

[34] *Road Vehicles–Controller Area Network (CAN)–Part 4: Time-Triggered Communication*, ISO 11898–4, 2004.

[35] *CAN With Flexible Data-Rate Specification, Version 1.0*, CANFD Standard, Robert Bosch GmbH, Gerlingen, Germany, 2012.

[36] J. Ray and P. Koopman, "Efficient high hamming distance CRCs for embedded networks," in *Proc. IEEE Int. Conf. Depend. Syst. Netw.*, Philadelphia, PA, USA, 2006, pp. 3–12.

[37] M. Short and M. J. Pont, "Fault-tolerant time-triggered communication using CAN," *IEEE Trans. Ind. Informat.*, vol. 3, no. 2, pp. 131–142, May 2007.

[38] K. Tindell, A. Burns, and A. J. Wellings, "Calculating controller area network (CAN) message response times," *Control Eng. Pract.*, vol. 3, no. 8, pp. 1163–1169, 1995.

[39] L. Casparsson *et al.*, "Volcano-a revolution in on-board communications," AB Volvo, Gothenburg, Sweden, Tech. Rep. 99-02-11 17:04, 1999.

[40] R. I. Davis *et al.*, "Controller area network (CAN) schedulability analysis: Refuted, revisited and revised," *Real-Time Syst.*, vol. 35, no. 3, pp. 239–272, 2007.

[41] B. Susanna, "Evaluation of static time analysis for volcano communication technologies AB," M.S. thesis, Dept. Comput. Sci. Eng., Malardalen Univ., Vasteras, Sweden, 2004.

[42] M. Hu *et al.*, "Holistic scheduling of real-time applications in time-triggered in-vehicle networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1817–1828, Aug. 2014.

[43] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst. TOPLAS*, vol. 4, no. 3, pp. 382–401, 1982.

[44] B. Pattanaik and S. Chandrasekaran, "Safety reliability enhancement in fault tolerant automotive embedded system," *Int. J. Innovat. Technol. Explor. Eng. (IJITEE)*, vol. 2, no. 2, pp. 63–68, 2013.

[45] G. Buja, J. R. Pimentel, and A. Zuccollo, "Overcoming babbling-idiot failures in CAN networks: A simple and effective bus guardian solution for the FlexCAN architecture," *IEEE Trans. Ind. Informat.*, vol. 3, no. 3, pp. 225–233, Aug. 2007.

[46] B. Hall *et al.*, "ESCAPE CAN Limitations," SAE International, Warrendale, PA, USA, Tech. Paper 2007-01-1487, Detroit, MI, USA, 2007.

[47] A. Ballesteros, M. Wagner, and D. Zobelz, "SOAcom: Designing Service communication in adaptive automotive networks," in *Proc. 8th IEEE Int. Symp. Ind. Embedded Syst. (SIES'13)*, Porto, Portugal, 2013, pp. 270–279.

[48] J. Park *et al.*, "Designing real-time and fault-tolerant middleware for automotive software," in *Proc. IEEE Int. Joint Conf. SICE-ICASE*, Busan, Korea (South), 2006, pp. 4409–4413.

[49] P. Koopman, "The FlexRay protocol—Significant material drawn from FlexRay specification version 2.0, June, 2004," Elect. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, Nov. 2015 [Online]. Available: http://www.ece.cmu.edu/~ece649/lectures/23_flexray.pdf, accessed on Feb. 03, 2016.

[50] R. Cummings, "Easing the transition of system designs from CAN to FlexRay," SAE International Warrendale, PA, USA, Tech. Paper 2008-01-0804, 2008.

[51] C. P. Quigley *et al.*, "An investigation into cost modelling for design of distributed automotive electrical architectures," in *Proc. IEEE 3rd Inst. Eng. Technol. Conf.*, London, U.K., 2007, pp. 1–9.

[52] T. Costlow, "FlexRay, Ethernet vie for role as safety systems share data," SAE International, Warrendale, PA, USA, 2014 [Online]. Available: http://articles.sae.org/12862/, accessed on Nov. 09, 2014.

[53] A. Schedl, "Goals and architecture of FlexRay at BMW," presented at the Vector FlexRay Symp., Stuttgart, Germany, 2007.

[54] M. Heinz, V. Höss, and K. D. Müller-Glaser, "Physical layer extraction of FlexRay configuration parameters," in *Proc. IEEE/IFIP Int. Symp. Rapid Syst. Prototyping*, Paris, France, 2009, pp. 173–180.

[55] *FlexRay Communication System Protocol Specification, V3.0.1.*, FlexRay Consortium, 2010.

[56] B. Tanasa *et al.*, "Schedulability analysis for the dynamic segment of FlexRay: A generalization to slot multiplexing," in *Proc. IEEE 18th Real Time Embedded Technol. Appl. Symp.*, Beijing, China, 2012, pp. 185–194.

[57] K. Jang *et al.*, "Design framework for FlexRay network parameter optimization," *Int. J. Automot. Technol.*, vol. 12, no. 4, pp. 589–597, 2011.

[58] M. Lukasiewycz *et al.*, "FlexRay schedule optimization of the static segment," in *Proc. 7th IEEE/ACM Int. Conf. Hardw./Softw. Codes. Syst. Synth.*, New York, NY, USA, 2009, pp. 363–372.

[59] Y. Hua, X. Liu, and W. He, "HOSA: Holistic scheduling and analysis for scalable fault-tolerant FlexRay design," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 1233–1241.

[60] M. Kang, K. Park, and B. Kim, "A static message scheduling algorithm for reducing FlexRay network utilization," in *Proc. IEEE Int. Symp. Ind. Electron. (ISIE'09)*, Seoul, Korea, 2009, pp. 1287–1291.

[61] B. Vermeulen *et al.*, "FlexRay switch," *ATZelektronik Worldw.*, vol. 5, no. 6, pp. 32–36, 2010.

[62] T. Schenkelaars, B. Vermeulen, and K. Goossens, "Optimal scheduling of switched FlexRay networks," in *Proc. IEEE Des. Autom. Test Eur. Conf. Exhib. (DATE'11)*, Dresden, Germany, 2011, pp. 1–6.

[63] *FlexRay Communications System Electrical Physical Layer Specification, Version 3.0.1.*, FlexRay Consortium, 2010.

[64] P. Koopman, "Software and digital systems program - data integrity techniques," Electr. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, Oct. 2013 [Online]. Available: https://users.ece.cmu.edu/~koopman/pubs/01oct2013_koopman_faa_final_presentation.pdf, accessed on Feb. 03, 2016.

[65] W. Li *et al.*, "Optimizations of an application-level protocol for enhanced dependability in FlexRay," in *Proc. IEEE Des. Autom. Test Eur. Conf. Exhib. (DATE'09)*, Nice, France, 2009, pp. 1076–1081.

[66] J. Formann and K. Echtle, "Efficient acknowledgement and retransmission techniques for bus-systems," in *Proc. 26th Int. Conf. Archit. Compu. Syst. (ARCS'13)*, Prague, Czech Republic, 2013, pp. 1–8.

[67] K. Klobedanz *et al.*, "Self-reconfiguration for fault-tolerant FlexRay networks," in *Proc. 14th IEEE Int. Symp.*, Newport Beach, CA, USA, 2011, pp. 207–216.

[68] R. Bouhouch *et al.*, "DDS on top of FlexRay vehicle networks: Scheduling analysis," *Int. J. Comput. Sci. Artif. Intell.*, vol. 3, no. 1, pp. 10–26, Mar. 2013.

[69] P. Hank, T. Suermann, and S. Müller, "Automotive Ethernet, A holistic approach for a next generation in-vehicle networking standard," in *Proc. IEEE Adv. Microsyst. Automot. Appl.*, Berlin, Heidelberg, 2012, pp. 1076–1081.

[70] ABI Research. (2014). *Ethernet In-Vehicle Networking to Feature in 40% of Vehicles Shipping Globally by 2020*, London, U.K. [Online]. Available: https://www.abiresearch.com/press/ethernet-in-vehicle-networking-to-feature-in-40-of, accessed on Nov. 09, 2014.

[71] H. T. Lim, L. Völker, and D. Herrscher, "Challenges in a future IP/Ethernet-based in-car network for real-time applications," in *Proc. IEEE 48th Des. Autom. Conf. (DAC'11)*, San Diego, CA, USA, 2011, pp. 7–12.

[72] H.T. Lim, K. Weckemann, and D. Herrscher, "Performance study of an in-car switched Ethernet network without prioritization," in *Communication Technologies for Vehicles*, New York, NY, USA: Springer, 2011, pp. 165–175.

[73] The OPEN Alliance (One-Pair Ether-Net) Special Interest Group (SIG). [Online]. Available: http://opensig.org/, accessed on Nov. 09, 2014.

[74] M. Sauerwald, "CAN bus, Ethernet, or FPD-Link: Which is best for automotive communications?," *Texas Instrument Analog Appl. J.*, vol. 1Q, pp. 20–22, 2014 [Online]. Available: http://www.ti.com/lit/an/slyt560/slyt560.pdf, accessed on Feb. 04, 2016.

[75] IEEE P802.3bp 1000BASE-T1 PHY Task Force [Online]. Available: http://ieee802.org/3/bp/, accessed on Nov. 09, 2014.

[76] *IEEE Standard for Local and Metropolitan Area Networks–Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks*, IEEE Standard SA-802.1AS, 2011.

[77] *IEEE Standard for Local and Metropolitan Area Networks–Audio Video Bridging (AVB) Systems*, IEEE Standard SA-802.1BA, 2011.

[78] *Time-Triggered Ethernet*, AS6802, 2011.

[79] *IEEE Standard for Local and Metropolitan Area Networks–Virtual Bridged Local Area Networks Amendment 14: Stream Reservation Protocol (SRP)*, IEEE Standard SA-802.1Qat, 2010.

[80] *IEEE Standard for Local and Metropolitan Area Networks–Virtual Bridged Local Area Networks Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams*, IEEE Standard SA - 802.1Qav, 2009.

[81] L. L. Bello, "Novel trends in automotive networks: A perspective on Ethernet and the IEEE Audio Video Bridging," in *Proc. IEEE Emerg. Technol. Fact. Autom. (ETFA'14)*, Barcelona, Spain, 2014, pp. 1–8.

[82] T. Steinbach *et al.*, "Tomorrow's in-car interconnect? A competitive evaluation of IEEE 802.1 AVB and time-triggered Ethernet (AS6802)," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall'12)*, Quebec, Canada, 2012, pp. 1–5.

[83] V. Schmidt *et al.*, "Evaluation of numerical bus systems used in rocket engine test facilities," presented at Ground-Based Space Facil. Symp., Paris, France, 2013.

[84] G. Alderisi, G. Patti, and L. L. Bello, "Introducing support for scheduled traffic over IEEE audio video bridging networks," in *Proc. IEEE 18th Conf. Emerg. Technol. Fact. Autom. (ETFA'13)*, Cagliari, Italy, 2013, pp. 1–9.

[85] L. L. Bello, G. Alderisi, and G. Patti. *Introducing Support for Time-Sensitive Traffic Over Ethernet Switches: The Case of the IEEE Audio Video Bridging* [Online]. Available: https://ece.uwaterloo.ca/~sfischme/rate/S3P3.pdf, accessed on Nov. 09, 2015.

[86] L. Zhao *et al.*, "Improving worst-case latency analysis for rate-constrained traffic in the time-triggered Ethernet network," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1927–1930, Nov. 2014.

[87] R. Santos *et al.*, "Improving the efficiency of Ethernet switches for real-time communication," in *Proc. 1st Int. Workshop Adapt. Resour. Manage.*, Stockholm, Sweden, Apr. 2010.

[88] P. Koopman, "32-bit cyclic redundancy codes for internet applications," in *Proc. IEEE Int. Conf. Depend. Syst. Netw. (DSN'02)*, Washington, DC, USA, 2002, pp. 459–468.

[89] O. Kleineberg, P. Frohlich, and D. Heffernan, "Fault-tolerant audio and video bridging (AVB) Ethernet: A novel method for redundant stream registration configuration," in *Proc. IEEE 17th Conf. Emerg. Technol. Fact. Autom. (ETFA'12)*, Kraków, Poland, 2012, pp. 1–8.

[90] W. Steiner *et al.*, "TTEthernet dataflow concept," in *Proc. IEEE 8th Int. Symp. Netw. Comput. Appl. (NCA'09)*, Cambridge, MA, USA, 2009, pp. 319–322.

[91] M. Rahmani, B. Muller-Rathgeber, and E. Steinbach, "Error detection capabilities of automotive network technologies and Ethernet—A comparative study," in *Proc. IEEE Intell. Veh. Symp.*, Istanbul, Turkey, 2007, pp. 674–679.

[92] M. Armbruster *et al.*, "Ethernet-based and function-independent vehicle control-platform: Motivation, idea and technical concept fulfilling quantitative safety-requirements from ISO 26262," in *Advanced Microsystems for Automotive Applications*, New York, NY, USA, Springer, 2012, pp. 91–107.

[93] N. Navet *et al.*, "Trends in automotive communication systems," *Proc. IEEE*, vol. 93, no. 6, pp. 1204–1223, Jun. 2005.

[94] A. Bouard *et al.*, "Driving automotive middleware towards a secure IP-based future," in *Proc. IEEE 10th Conf. Embedded Secur. Cars (ESCAR'12)*, Berlin, Germany, Nov. 2012.

[95] G. M. Garner *et al.*, "IEEE 802.1 AVB and Its application in carrier-grade Ethernet [Standards Topics]," *IEEE Commun. Mag.*, vol. 45, no. 12, pp. 126–134, Dec. 2007.

[96] G. Alderisi *et al.*, "Simulative assessments of IEEE 802.1 Ethernet AVB and time-triggered Ethernet for advanced driver assistance systems and in-car infotainment," in *Proc. IEEE Veh. Netw. Conf. (VNC'12)*, 2012, pp. 187–194.

[97] B. Engelmann, "MOST150-development and production launch from an OEM's perstective," presented at the 11th MOST Interconnectivity Conf. Asia, Seoul, Korea, 2010.

[98] A. Grzemba, *MOST: The Automotive Multimedia Network, from MOST25 to MOST150*. Poing, Germany: Franzis Verlag GmbH, 2011.

[99] E. Zeeb, "Optical data bus systems in cars: Current status and future challenges," in *Proc. IEEE 27th Eur. Conf. Opt. Commun. (ECOC'01)*, Amsterdam, The Netherlands, 2001, vol. 1, pp. 70–71.

[100] S. Poferl, M. Becht, and P. De Pauw, "150 Mbit/s MOST—The Next Generation automotive infotainment system," in *Proc. IEEE 12th Int Conf. Transparent Opt. Netw. (ICTON'10)*, Munich, Germany, 2010, pp. 1–2.

[101] "MOST Cooperation," in *MOST Informative*. Karlsruhe, Germany: MOST Cooperation, 2014, no. 10.

[102] A. Sumorek and M. Buczaj, "New elements in vehicle communication 'Media Oriented Systems Transport' protocol," *Teka Kom. Motoryz. Energ. Rol.*, vol. 12, no. 1, pp. 275–279, 2012.

[103] M. Wolf, *Security Engineering for Vehicular IT Systems: Improving the Trustworthiness and Dependability of Automotive IT Applications*, 1st ed. Wiesbaden, Germany: Vieweg+Teubner Verlag, 2009.

[104] S. Lee *et al.*, "MOST network system supporting full-duplexing communication," in *Proc. IEEE 14th Int. Adv. Commun. Technol. (CACT'12)*, PyeongChang, Korea, 2012, pp. 1271–1275.

[105] G. Dannhäuser, W. Franz, and W. Rosenstiel, "MOST and AVB: Two candidates for next generation automotive infotainment networks–A comparison," in *Elektronik Automotive Special Issue MOST*. Stuttgart, Germany: ZENIT Press Distribution GmbH, 2013.

[106] Vector. (2014). *Media Oriented Systems Transport (MOST)* [Online]. Available: https://vector.com/vi_most_en.html, accessed on Nov. 09, 2014.

[107] T. Steinbach, F. Korf, and T. C. Schmidt, "Real-time Ethernet for automotive applications: A solution for future in-car networks," in *Proc. IEEE Int Conf. Consum. Electron-Berlin (ICCE-Berlin'11)*, Berlin, Germany, 2011, pp. 216–220.
[108] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 1–14, Apr. 2014.
[109] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Kongresshaus, Germany, 2011, pp. 528–533.
[110] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, San Francisco, CA, USA, 2011, pp. 77–92.
[111] H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks," in *Proc. 1st Int. Workshop Veh. Commun. Sens. Comput. (VCSC'12)*, 2012, pp. 12–17.
[112] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.
[113] J. Harding and G. Powell, "Vehicle-to-vehicle communications: Readiness of V2V technology for application," National Highway Traffic Safety Admin., Washington, DC, Tech. Rep. DOT HS 812 014, Aug. 2014.
[114] M. Wolf, A. Weimerskirch, and C. Paar, "Secure in-vehicle communication," in *Embedded Security in Cars*, New York, NY, USA: Springer, 2006, pp. 95–109.
[115] T. Kiravuo, M. Sarela, and J. Manner, "A survey of Ethernet LAN security," *IEEE Commun. Surv. Tuts.*, vol. 15, no. 3, pp. 1477–1491, Jul. 31, 2013.
[116] A. Happel, "Secure communication for CAN FD," *CAN Newsletter*, 2014.
[117] S. Shreejith and S. A. Fahmy, "Zero latency encryption with FPGAs for secure time-triggered automotive networks," in *Proc. Int. Conf. Field-Programm. Technol. (FPT'14)*, 2014, pp. 256–259.
[118] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proc. Workshop Embedded Secur. Cars*, 2004.
[119] A. Bogdanov *et al.*, "ALE: AES-based lightweight authenticated encryption," in *Proc. 21st Int. Workshop Fast Software Encryption*, London, UK, 2014, pp. 447–466.
[120] G. Bansod, N. Raval, and N. Pisharoty, "Implementation of a new lightweight encryption design for embedded security," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 1, pp. 142–151, Jan. 2015.
[121] A. Groll and C. Ruland, "Secure and authentic communication on existing in-vehicle networks," in *Proc. IEEE Intell. Veh. Symp.*, 2009, pp. 1093–1097.
[122] A. H. G. Yousef, "Methods of securing in-vehicle networks," Ph.D. dissertation, Faculty Eng., Cairo Univ.; M.S. thesis, Electron. Commun. Eng., Faculty Eng., Cairo Univ., Giza, Egypt, 2013.
[123] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. IEEE Int. Conf. Cyber Secur.*, 2012, pp. 1–7.
[124] C. J. Szilagyi, "Low cost multicast network authentication for embedded control systems," Ph.D. dissertation, Elect. Comput. Eng., Carnegie Mellon Univ., Pittsburgh, PA, USA, 2012.
[125] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, "Lightweight authentication for secure automotive networks," in *Proc. Des. Autom. Test Eur. Conf. Exhib. (DATE'15)*, 2015, pp. 285–288.
[126] C.-W. Lin, Q. Zhu, and A. Sangiovanni-Vincentelli, "Security-aware mapping for TDMA-based real-time distributed systems," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. (ICCAD)*, San Jose, CA, USA, 2014, pp. 24–31.
[127] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC'11)*, 2012, pp. 302–318.
[128] M. Saed, S. Bone, and J. Robb, "Security concepts and issues in intra-inter vehicle communication network," in *Proc. Int. Conf. Secur. Manage. (SAM)*, 2014, p. 1.
[129] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[130] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 1–12, Dec. 2015.

Weiying Zeng (S'15) received the B.Eng. and M.A.Sc. degrees from China Agricultural University, Beijing, China, in 2007 and 2009, respectively, and the B.Ec. degree from Peking University, Beijing, China, in 2009. He is currently pursuing the Ph.D. degree in electrical engineering at the University of Windsor, Windsor, ON, Canada. He was with Beijing Automotive Group Co., Ltd. (BAIC Group), Beijing, China, from 2009 to 2013, primarily in charge of in-vehicle network design and test. His research interests include in-vehicle Ethernet networks, fault diagnostics, and optimization techniques for real-time systems.

Mohammed A. S. Khalid (M'87) received the Ph.D. degree in computer engineering from the University of Toronto, Toronto, ON, Canada, in 1999. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON, Canada. He has over 25 years of experience in teaching, research, and development in academia and industry. Before joining the University of Windsor in August 2003, he worked for 4 years as a Senior Member of Technical Staff in the Verification Acceleration R&D Group (formerly Quickturn), of Cadence Design Systems, based in San Jose, CA, USA. He has authored several papers in these areas and holds a U.S. patent in the area of architecture of reconfigurable systems. His research interests include architecture and CAD for field programmable chips and systems, reconfigurable computing, embedded system design, and hardware description languages.

Sazzadur Chowdhury (S'98–M'03) received the M.A.Sc. and the Ph.D. degrees in electrical engineering from the University of Windsor, Windsor, ON, Canada, in 2000 and 2003, respectively. He is a Professional Engineer in the province of Ontario. His research interests include MEMS and current focus is to develop MEMS-based advanced multispectral (ultrasonic and microwave) transducer arrays that can be used in the areas of medical diagnostics, automotive safety, and security applications, 3-D packaging and integration of dies of diverse origin technologies. He was the recipient of several awards and grants in Canada for research in the area of MEMS. He is serving as the Member Representative of the University of Windsor in CMC Microsystems, a not-for-profit corporation delivering a national research infrastructure support program to microsystems researchers in universities across Canada.