

Vehicle area networks form the backbone of future intelligent transportation systems.

BY MIAD FAEZIPOUR, MEHRDAD NOURANI,
ADNAN SAEED, AND SATEESH ADDEPALLI

Progress and Challenges in Intelligent Vehicle Area Networks

MUCH ATTENTION HAS recently been paid to smart vehicle research to assist drivers and ultimately revolutionize the way vehicles, road sensors, and drivers communicate in the future. The key objective is to improve driver and vehicle safety. The National Transportation Safety Board reports that U.S. highways on average experience 43,300 fatalities per year. Every day, more than 16,000 crashes occur on U.S. highways, mainly due to driver error, poor judgment, drowsiness, or distraction.⁹ The U.S. National Highway Traffic Safety Administration estimates that in the U.S. alone, approximately 100,000 crashes (about 2% of all) each year are caused primarily by driver drowsiness or fatigue.^{9,28} Thus, incorporating automatic active

vehicle safety techniques such as driver fatigue detection/warning mechanisms and other driver-assist tools into vehicles may significantly help in preventing accidents and increase crash survivability.

This article surveys the main innovations in vehicle area networks (VAN) featuring driver safety. We mainly focus on the recent developments of intelligent transportation systems (ITS) for intra-vehicle and inter-vehicle-area-networks to assist driver safety:

Intra (In-Vehicle) VAN. Intelligent intra-vehicle systems are becoming necessary components of smart vehicle system research. Intra-vehicle networks deal with the data communication network of onboard equipment (OBE) for assessing a driver's behavior or a vehicle's performance. Two vehicle safety techniques—*passive* and *active*—are currently being employed and devised in vehicles. Passive vehicle safety includes a set of tools or devices such as seatbelts or air bags that improve safety in the event of an accident. On the other hand, active vehicle safety techniques consist of a variety of techniques such as on-board driver assistance tools (for example, driver fatigue detection), lane-keeping or congestion control tools and many more,

» key insights

- **Intelligent transportation systems (ITS) in general and vehicle area networks (VAN), in particular, are expected to grow with the ultimate goal of achieving an accident-free driving environment.**
- **The key requirement of VAN is an efficient wireless intra- and inter-vehicle communication mechanism to collect and exchange data among the driver, car, and road infrastructure.**
- **Analytics play a major role in the future network of smart vehicles to quickly detect dangerous situations, alert the driver and/or police, and prevent accidents.**
- **Such goals require multidisciplinary analytics from signal processing (for example, conditioning sensor's raw data), to machine learning (such as a driver's behavioral analysis) and data mining (traffic pattern database).**

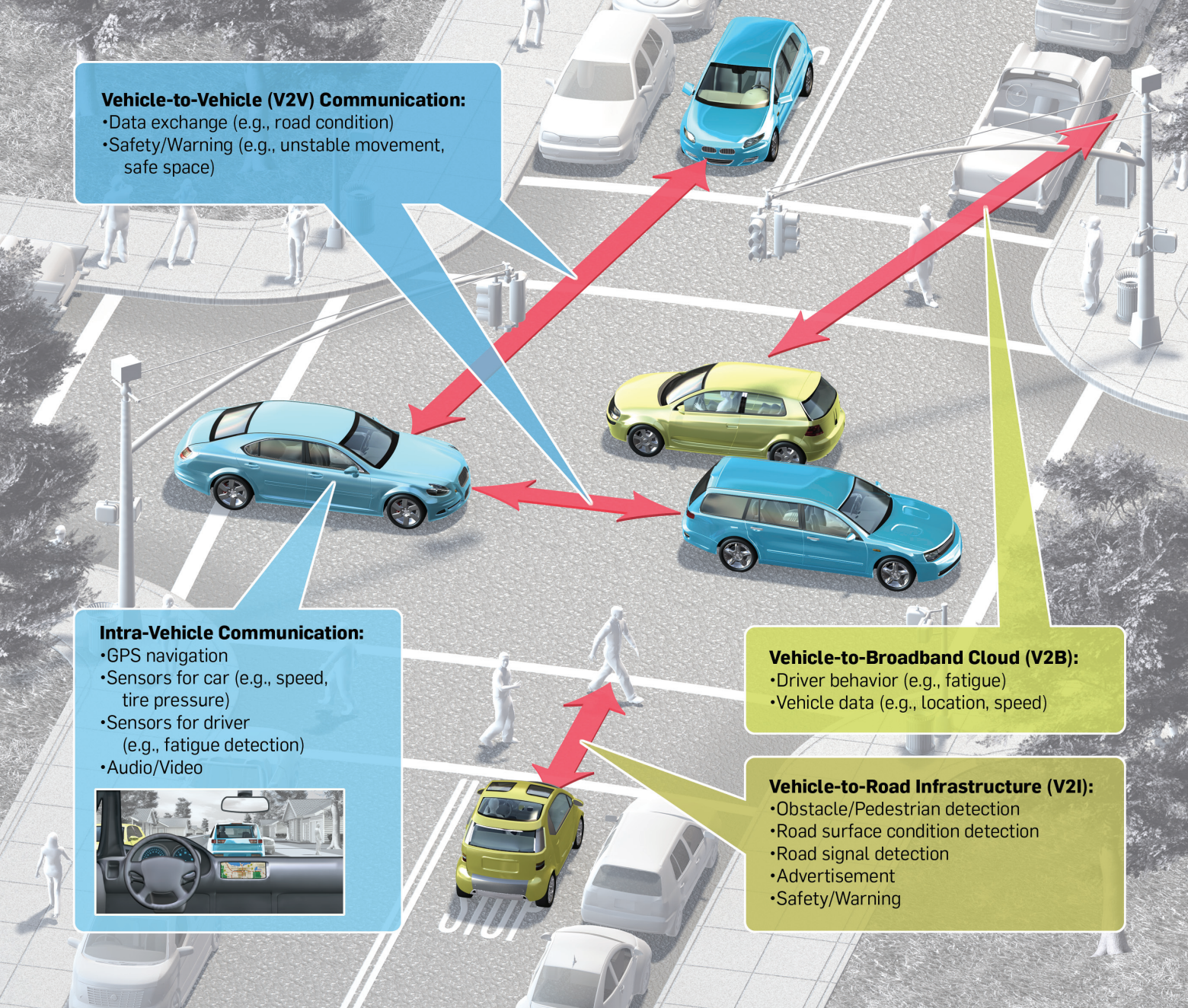


Figure 1. Central vision of VAN.

which altogether proactively try to minimize the chance of car accidents.

Inter VAN. Inter-vehicle communication is another key element of VAN that includes vehicle-to-vehicle (V2V), vehicle-to-broadband cloud (network) communication (V2B), and vehicle-to-roadside-infrastructure communication (V2I) using roadside units (RSU).

An intelligent VAN is a network of vehicles that interact with one another and with infrastructure to transmit and receive data. Various interactions among participating elements are shown in Figure 1 and may include lane-keeping signals, obstacle detection, adaptive cruise control, navigation data, driver status, and so on. This provides automatic driver assistance

that not only improves driver safety, but also creates a cooperative environment where the right information is provided at the right time. For example, drivers and vehicles can optionally exchange useful information such as weather/road conditions, traffic jam, or business/pleasure information such as shopping or dining deals as they travel along the same road. The ultimate goal is to provide an accident-free environment and move toward implementation of the *zero-accident car* by the help of vehicle area networks.¹²

There are several ongoing research and projects that aim at enhancing intelligent transportation systems. Partners for Advanced Transit and Highways (PATH), is a collaborative research

project between the California Department of Transportation (Caltrans) and the Institute of Transportation Studies (ITS) at the University of California at Berkeley along with other public and private institutions and agencies (www.path.berkeley.edu). It targets intelligent transportation systems development by applying advanced technology to particularly increase highway capacity, enhance public safety, and reduce traffic congestion, air pollution, and energy consumption.

The SafeTrip-21 (Safe and Efficient Travel through Innovation and Partnerships for the 21st Century; www.rita.dot.gov) initiative is another project sponsored by the U.S. Department of Transportation (DOT). It is part of

the IntelliDrive program in which a consortium of carmakers conducts demonstrations and operational tests to speed up the deployment of communication/navigation technologies that improve transportation safety and mobility features.

Simultaneously in Europe, several institutes and organizations work on intelligent transportation system development and vehicle-network connectivity. The Cooperative Vehicle Infrastructure Systems (CVIS) that is part of the European Commission was built upon the foundation of V2V and V2I communications for increasing the efficiency of road network/transportation (www.cvisproject.org). The Complex Embedded Automotive Control Systems (CEmACS) is a research collaboration among some universities in the U.K., Germany, Sweden, Norway and Ireland that work on complex vehicle dynamics and control for active vehicle safety (www.hamilton.ie/cemacs).

In Asia, there are several ongoing activities that focus on intelligent transportation systems. The Tokyo Smartway project aims at developing intelligent roads for the 21st century by enabling automated driving using ITS technologies. The Electronic Road Pricing (ERP2) project in Singapore focuses on constructing a comprehensive road network by integrating in-vehicle units for electronic payments of various vehicle or road transactions.

Electric vehicles have been prototyped and some commercialized in the past several years. Next-generation, grid-based electric vehicles are currently under investigation to increase the power and fuel efficiency of future vehicles. In this platform, a smart electric grid is formed where

vehicles draw energy to start their motors. Future electric vehicles (for example, electric trolley bus) will be part of VAN and will not only draw energy from the smart grid, but will also store back energy to the grid and allow various data communication.

As vehicular networks are expected to become somewhat ubiquitous by 2016, security elements for these types of networks would also come into the picture. It is clear that false or unauthorized data communication or attacks leading to denial of service within such a VAN could cause devastating results compromising the driver judgment and/or safety.

VAN calls for collaboration among interdisciplinary areas in electrical, computer, biomedical, telecommunication, and mechanical engineering to address a variety of issues. This article provides a comprehensive survey in the main communication and networking components of VAN. We survey the recent progress and advances in vehicle area networks and their constructing components, particularly in-vehicle VAN, V2V, V2B, V2I, standards, and the security and privacy of VAN. Additionally, an overview of the top challenges in each element of this emerging network is highlighted and can potentially inspire researchers in the field.

In-Vehicle VAN

In-Vehicle Data Collection/Analysis Systems. Intelligent intra-vehicle communication systems for detecting a vehicle’s performance and especially a driver’s fatigue and drowsiness, is critical for driver and public safety. This is becoming a major stream of research in the area of intelligent vehicle systems. Intelligent in-vehicle

systems, mainly, onboard equipment (OBE) collect information from the driver or vehicle and analyze and classify the data collectively to predict or detect driver fatigue.

Machine learning techniques are extensively used for such data classification.⁴⁵ This platform collects standard vehicle information such as the speed, pressure on the brake or gas pedal, steering wheel rotation, and global positioning system (GPS) routing.⁴⁴

In addition to standard vehicle information, driver behavioral information such as facial expression (for example, blink rate, yawning, eyebrow raise, chin drop, head movements) can be collected and analyzed.⁴³ Even physiological signals such as heart-rate variability and electroencephalogram (EEG) signal behavior can be sampled to determine the drowsiness (non-alert) level of the driver.⁸ Researchers have reported there is a high correlation between the level of alertness and the power signal in the alpha and theta band of the EEG signal.⁵⁶

Other physiological signals such as electrocardiogram (ECG) signal (for example, using wireless wrist-mounted⁵ or seat-installed sensors), electrooculogram (EOG), electromyogram (EMG), blood pressure (BP), and sweating on the palm (for example, when driver touches the steering wheel) could be used for fatigue detection and sleep episode prediction. In such a platform, sensors and audio/video (such as microphone/camera) can be used for collecting signals for this purpose. This platform itself is an in-vehicle network that engages potentially a large number of sensors in the car to collect vehicle or driver information. It may optionally transmit this data to a monitoring data center for further processing and receive feedback, for example, a warning signal, for the driver.

In-Vehicle Communication Network. A specialized communication network with the ability to operate in a harsh environment is required to interconnect all OBEs. Controller Area Network (CAN) is the earliest serial communication protocol developed for this purpose in 1986 that allows data rates up to 500kbps and distances less than 40m (www.can-cia.org). Local Interconnect Network (LIN) has been used since 1999 for ultra low cost and low

Table 1. Common in-vehicle protocols.

	CAN	LIN	FlexRay	MOST	J1850
Application	soft real-time	low cost low speed	hard real-time	multimedia	diagnostics
Bandwidth	500kbps	19.6kbps	10Mbps	24.8Mbps	41.6kbps
Control	multi-master	single-master	multi-master	timing-master	multi-master
Bus Access	CSMA/CA	Polling	TDMA	TDM/CSMA	CSMA/NDA
Redundancy	No	No	Yes	No	No
Physical Layer	Electrical	Electrical	Electrical Optical	Optical	Electrical

speed (19.2kbps) communication to units (door locks, power windows, side mirrors) that do not require the complexity or higher bandwidth of CAN (www.lin-subbus.de).

FlexRay is a recent protocol that provides deterministic and fault-tolerant communication up to 10Mbps and is expected to replace CAN in the future (www.flexray.com). For multimedia application within the vehicle (audio, video, telephony, navigation) that require even higher bandwidths, Media Oriented Systems Transport (MOST) protocol has been in use since 2001 that can provide 24.8Mbps over optical fiber (www.mostcooperation.com).

To monitor vehicle emission and health of different OBEs, the Environmental Protection Agency in the U.S. requires every passenger vehicle sold after 1996 to provide a standard 16-pin connector (J1962) and a single wire protocol (J1850) for On-Board Diagnostics (OBD). J1850 protocol is part of OBD-II defined by Society of Automotive Engineers (SAE) International (www.sae.org). Table 1 lists the main features of most commonly used in-vehicle protocols.

Top Challenges

Car-Suited Physiological Sensors. The success of driver behavioral analysis depends on accurate and robust data collection. While some preliminary works were reported in the literature,^{16,43} implementing accurate sensors (for example, EEG, ECG, EMG, EOG, BP, Sweat) and proper mounting, for example, to be none or minimally visible, requires more attention. Novel applications may include employing off-the-shelf sensors/devices that can communicate with communication gadgets such as cellphones as a gateway to send or receive data to and from the monitoring data center.

In-Vehicle Data Analysis. Certain data processing may be needed in vehicles because of urgency or due to lack of connection to the base. This challenge deals with identifying such data (for example, related to fatigue) and processing it using a mix of digital signal processing and machine learning techniques that can run on embedded processors. Such data analysis must go much beyond what has been reported in the literature,^{26,43} as the



The ultimate goal is to provide an accident-free environment and move toward implementation of the zero-accident car by the help of vehicle area networks.



safety of driver and vehicle may heavily depend on this analysis.

Vehicle Controller Area Network. The vehicle controller area network (CAN) is a serial bus communications protocol that allows access to the vehicle internal system through an embedded networked control system.²⁰ Other OBEs, sensors, and devices should be integrated within vehicle CAN to increase the efficiency of in-vehicle VAN. Wireless sensors planted in the car (for example, temperature, tire-road friction, stability control, brake force) and reporting data to the central system is one of the challenges in CAN.³³

Various aspects of this challenge includes: potentially having large number (tens and even perhaps hundreds) of such sensors; low-power circuit design and management to survive several years of operation; and reliability to ensure robust work in the harsh and/or wireless environments. Other challenges of CAN include reliable communication with actuators such as cruise control, and alert messages to the driver. Another question is what actuators can be automated vs. providing drivers with alert messages while requiring manual (drivers') intervention. In addition, wireless extensions to the in-vehicle sub-networks have performance degradation in terms of reliability of communication compared to the wired networks. The challenges lie in achieving high communication reliability while interacting with other components of VAN.

Generic Plug and Play Gateway. As the interest for in-vehicle connectivity is growing, a single preferably wireless platform is needed to connect all the in-vehicle and mobile devices. Security and connectivity can be handled by the gateway, thereby extending the usable life of equipment and eliminating the need for a dedicated modem for every device.

Existing Solutions

Intel In-Vehicle Devices. In 2008, Intel Corporation introduced the Intel Atom processor to enhance in-vehicle *infotainment* (IVI) solutions (www.intel.com). This processor is a low-power, small-footprint and cost-efficient design ideal for in-vehicle operating conditions. In particular, Intel has closely collaborated with Volkswagen, BMW,

and Harman/Becker Automotive Systems to integrate various communications and computing technologies to support digital media and IVI features.

Software for Automotives. There is a non-profit industry alliance called GENIVI (www.genivi.org) to drive widespread adoption of open source in-vehicle infotainment software framework. In addition, commercial companies like QNX (www.qnx.com) provide software for automotives that can be used in a variety of vehicle infotainment applications.

Vehicle-to-Vehicle Communication

V2V communication can provide a data exchange platform, expand driver assistance, and facilitate active safety vehicle system development. Driver assistance is provided using cooperative communication among vehicles to adaptively broadcast and/or share information or warning messages for the driver. This can be further customized for specific groups of people in the community such as elderly drivers. Lane keeping,⁷ steering control and parking assistance,¹¹ obstacle detection, inter-vehicle spacing, and driver/vehicle exchanging optional or useful information while traveling along the same road,^{22,43} fall in V2V communication category.

Wireless connectivity, including wireless LAN localization can be dedicated for this type of VAN communication. When driving, vehicles can observe various wireless signals such as GSM, cell tower signal, AM/FM radio, radar signals, GPS, and wireless LAN signals. In particular, differential GPS has become prominent to determine more accurate coordinates for localization.⁴⁹ In wireless LAN, many access points emit beacons periodically. If a vehicle enters a wireless LAN-available area, the vehicle can get beacons' information such as service-set identifier (SSID), MAC address (BSSID), signal strength and can estimate its position in relation to the access point.²³ In addition, a vehicle's speed can be estimated by comparing the difference in signal strength distribution among other mobilities.⁴¹

In this platform, cellular/WiFi devices can be used for both short and long range inter-vehicle communication. Wireless connections that meet

The success of driver behavioral analysis depends on accurate and robust data collection.

the power and bandwidth requirements, such as GPRS used in 3G cellular communication systems, 4G ultra high speed mobile broadband such as long-term evolution (LTE) mobile broadband, and mobile WiFi hotspot provide standard connections for multiple vehicles and their devices.

Top Challenges

Hardware/Software/Firmware. Each one of applications mentioned here requires different sensors, processing units, and even actuators. There are already some products in the market, for example, lane-passing alarm in class W163-M Mercedes Benz, back radars systems (www.tradekey.com/ks-back-radar), and tire sensors in Fiat (see Table 2). However, this field is far from mature. In fact, the sky is the limit for innovative systems and gadgets that fit into consumer's budget and need.

Cooperative Communication. Cooperative or cognitive communications among vehicles are presently in the infancy phase. The goal is to facilitate data exchange and create a highly informative network.⁴² The LTE connected car initiative and the iDrive system with Internet connectivity by Toyota, BMW, and other participants have been recently introduced. However, development of a heterogeneous network architecture that enables wire speed, robust, seamless and secure communication is an ongoing effort. There are many open questions that demand answers including: What one vehicle can or cannot broadcast or receive and how to format the packets for more effective distribution? Such distribution is, in particular, challenging due to the time limit (order of several seconds at most) that vehicles are within access range of each other.

Existing Solutions

Vehicle Telematic. Atheros Communications Inc. is a developer in vehicular communication technology (www.atheros.com). Atheros has implemented the AR5000 chipset, which is a product specifically designed to target telematic applications such as vehicle safety, vehicle data exchange, traffic congestion management, more innovative electronic/automated tolling (for example, RFID-based tags,

mileage-based toll collection), and so on. AR5000-based products have been tested in multipath propagation environments for vehicles traveling up to 120mph with V2V distances of around 400m. The datasheet of these products reported packet error rates of less than 0.1%, while consistently maintaining links even under heavy traffic scenarios.

INRIX is another telematics service provider that offers real-time traffic information to build up an intelligent routing engine to aid smart driving (www.inrix.com). There are other telematics services such as OnStar, GM Mobility Assistance, and GM Goodwrench provided by General Motors (GM), the Hughes Telematics by Hughes, and the telematics services by Cross Country. These service providers offer various navigation, communication, and safety devices and services for (mostly rental) vehicles.

Vehicle-to-Cloud Communication

Vehicles communicating with a broadband cloud, for example, a monitoring data center in a VAN, opens a new door for many useful applications. Vehicles may communicate via wireless broadband mechanisms such as 3G/4G (HSI). Going forward, high-speed 4G mobile broadband technologies such as LTE, 802.16m-based WiMAX achieving speed in excess of 100Mbps will be of high interest. Already, some car companies such as Nissan, Ford, and Toyota have taken steps toward vehicle-to-cloud connectivity. In particular, Toyota has announced partnership with Microsoft to offer cloud connectivity.⁵¹ With this research investment, Toyota plans to connect its cars to Microsoft's Azure cloud platform by 2015 to provide a telematics cloud solution.

This type of communication will specifically be useful for active driver assistance and vehicle tracking in network fleet management. In particular, the smartphones/gadgets could be used as a gateway in this platform to send/receive data to and from a central monitoring data centers connected to the broadband cloud.⁴ V2B networks can provide useful information in two ways:

► Outgoing data that may include: vehicle-centric information (for example,

speed, global positioning, routing, device functionality, and performance); and driver-centric information such as driver's specific behavior (for example, drowsiness, length of continuous driving), audio/video, and others. All of this data may be optionally forwarded to a central monitoring server for further analysis and storage.

► In-coming data that may include receiving data from a central office for various communications with driver or vehicle system.

Additional reasons to connect to the cloud may include infotainment, entertainment (for example, multimedia streaming); Internet; automotive as well as location-based services; and connecting to the car dealers and auto service centers, among others.

Vehicle communication with the broadband cloud can, to some extent, be considered as a subset of vehicle to road infrastructure communication, where the broadband cloud (for example, monitoring data center) is assumed to be part of the infrastructure.

Top Challenges

Communication Latency. There are questions such as what information to collect, what to filter, what to process in-vehicle, and what to send/receive to/from the data center, and so on. All these account for the V2B communication latency that should be addressed to improve the efficiency and preserve the real-time nature of the overall network.

Gateway. Design of a preferably uniform intelligent gateway using WiFi, cellular, and other broadband networks for plug-and-play devices and to

set up the network remains an open issue in V2B communication.

Data Processing. There are suggestions for leaving all or most of the data processing to the data center, as it can have unlimited computational power. Challenges lie in devising such processing data centers dedicated for this purpose. In addition, distributed vs. centralized data processing, and in-vehicle vs. in-data-center processing remain open research areas.

Fleet Management. Fleet management/monitoring includes challenging applications of V2B communication in which the cloud architecture should keep track of the activities of each vehicle within its network.

Security. In V2B, all sorts of security and privacy issues may be raised. It is essential to integrate data security and privacy features by complying with certain standards or devising time-efficient cryptography techniques for this purpose.

Vehicle-to-Roadside Infrastructure Communication

Vehicle-to-road communication for environmental sensing and monitoring is another interesting item in the menu of smart VAN research. This platform ultimately enables driver safety by providing the right information at the right time, such as speed limit, and weather condition information collected using various roadside sensors. This platform is capable of automatically informing the driver of hazardous road conditions. Sensed data of road surface and spacing can be transmitted to vehicles over inter-vehicle communication using the

Table 2. Driver-assistance systems available in the market.⁴³

System	Maker
Forward collision warning	Nissan
Adaptive Cruise Control (ACC)	Mitsubishi
Lane-keeping support	Nissan
Collision mitigation brakes	Honda
Low-speed ACC	Nissan
Night vision	Honda
Lane-passing alarm	Benz
Tire sensors	Fiat
Brake Assist with Navigation Link	Toyota
Blind-spot detection	BMW

5.9GHz dedicated short-range communication (DSRC).⁵⁴ For example, wet conditions of the road surface can be detected based on processing the polarized light from the road surface with a vision system.⁴³ Anticollision detection systems based on vehicle and obstacle spacing using adaptive cruise control is another vehicle-to-roadside communication application.^{18,54}

V2I communication enables real-time weather/traffic updates for the driver, which ultimately makes the transportation systems more informative. As one option, researchers in academia and industry have shown that the V2I transmitter can actually be placed on the vehicle's tire.²⁷

Top Challenges

Next Generation of Car Radars. While there are existing car radar solutions (for example, from Benz), the role of next-generation car radars is critical and its design and implementation is expected to have significant impact on V2I communication.

Prioritization. Since data processing would be from hundreds of nodes, prioritization, buffering, and queuing

techniques should be devised to maintain a robust and effective data communication link.

Existing Solutions

Radio-Frequency Identification (RFID) tags and receivers can be used to detect and alert the driver of obstacles or pedestrians. Authors in Ishida et al.²⁴ have implemented a system that uses RFID technology to warn drivers of vulnerable road users (VRU) such as pedestrians or bicyclists and their exact locations, especially at road intersections. Vulnerable road user communication is generally performed through RF-based communication and image processing techniques.³⁹ The overall system is a VAN that includes both V2V and V2I communications. The system consists of UHF-band active tags and transmits the tag ID as well as the position of the pedestrian to onboard equipment. Electromagnetic induction of a coil is used in the design to excite the active tag. This system not only alerts the driver of the presence of pedestrians, but also allows the drivers to locate the pedestrian to take proper action when approaching the road in-

tersection. The system also includes tag receivers for pedestrians themselves (for example, the elderly and/or the disabled) to be aware of vehicles near road intersections. Due to the relatively low range of communication in UHF band, repeaters have also been installed at roadside infrastructure to route the RFID tag information to vehicles. This is where V2I communication takes place. For the V2V communication, an inter-vehicle multihop broadcasting transmission function has also been designed to alert other vehicles outside the proximity of the RFID readers of the possible pedestrians on nearby intersections.

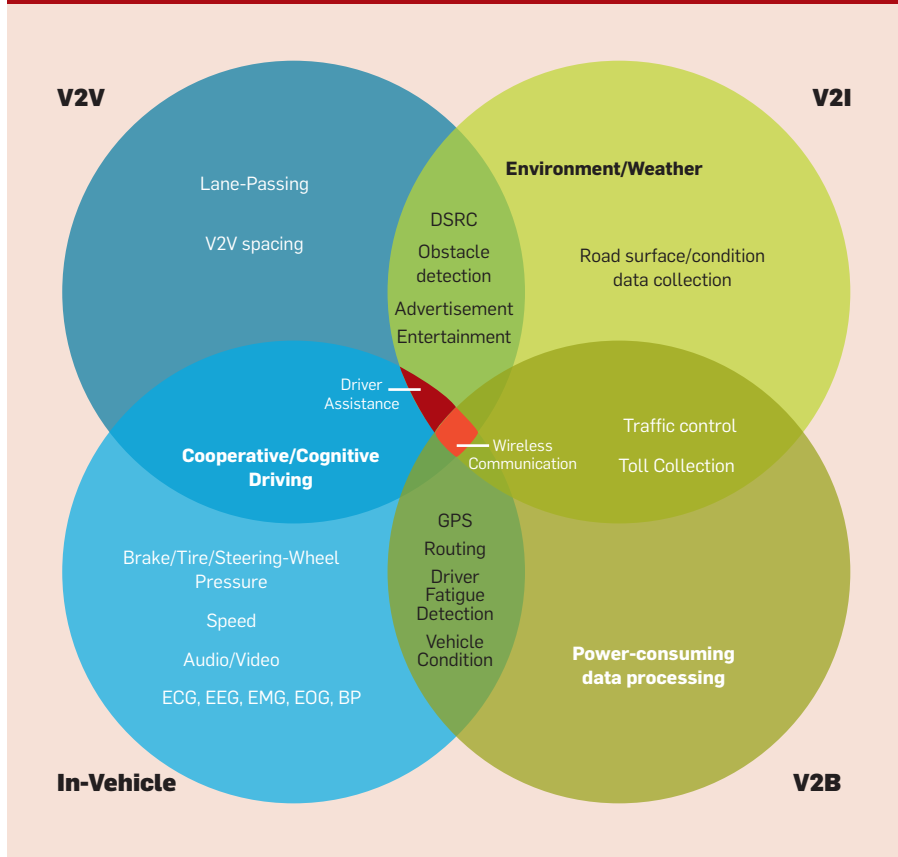
Having explained the main communication links in VAN, Figure 2 depicts the key functions of each. Certain functions and applications have multiple faces that need investigation as multidisciplinary research topics.

Communication Standards for VAN

Basically, vehicular network is a subclass of mobile ad hoc networks that require certain properties such as connectivity, coverage, broadcasting safety messages, or congestion control.⁵⁵ Communication protocols for VAN, in general, consist of defining the frequency allocation, physical and link layers, routing protocols, broadcasting and security algorithms.¹ Hence, vehicular networks should be designed based upon certain standards that define the communication architecture, protocols, messaging, management, hierarchy, and so on throughout the network. The main communication standards for VAN are outlined here.

The **IEEE 802.11p** standard draft, released in November 2010 and is still actively under development, is an amendment to the IEEE 802.11 standard. IEEE 802.11p aims to add wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS) applications.¹⁹ This standard defines the V2V and V2I communication protocols for high-speed vehicles and mainly addresses design challenges at the physical (PHY) level. In the U.S., the Dedicated Short Range Communications (DSRC) of 5.9GHz, that is, the licensed ITS band of 5.85–5.925GHz, is used for this purpose. The European Commission has also recently allocat-

Figure 2. VAN key components and functions.



ed 5.9GHz for V2V and V2I communication for vehicle safety applications that is highly compatible with the U.S. DSRC WAVE band, allowing the usage of similar antennas and wireless transceivers in the platform.

The IEEE 802.11p standard was designed on top of the ASTM E2213-03³ standard, which is a predecessor on vehicle-based communication networks. It includes the architecture for VAN to enable vehicle safety and non-safety transactions such as toll collection and traffic mapping. The goal in IEEE 802.11p is providing a framework to incorporate VANs throughout a nation's road infrastructure with sufficient V2V and V2I communication features deployable as needed.

A higher-layer standard, which IEEE 802.11p is based upon, is the **IEEE 1609** standard⁴⁶ providing ubiquitous vehicular communication among different automobile vendors and manufacturers. IEEE 1609 includes a family of standards for WAVE. It defines the architecture, organization, management structure, communication model, security mechanisms and physical access. These features, collectively, facilitate secure V2V and V2I wireless communication in a variety of applications including traffic management, active safety services, or automated tolling. IEEE 1609 includes a subset of standards, each particularly designed to address a specific purpose in WAVE:

IEEE P1609.1 is the resource manager that identifies the key components of the WAVE system architecture. It defines the communication formats such as command message and data storage formats and resources used among all nodes of the architecture. This standard also indicates that OBEs and mobile platforms are supported in WAVE.

IEEE P1609.2 addresses the security issues in WAVE by defining secure message formats. Basically, this standard takes care of secure message management by specifying how secure messages are processed once they are exchanged.

IEEE P1609.3 is the network protocol layer standard in WAVE that also supports secure message data exchange. In addition to defining network and transport layer services such as routing, this standard also provides a substitute for IPv6 by defining WAVE

short messages. This is WAVE-specific, and can be used by most applications. Moreover, the Management Information Base (MIB) for the WAVE protocol stack is also defined in this standard.

IEEE P1609.4 supports multichannel WAVE operations by providing extensions to the existing Media Access Control (MAC) in IEEE 802.11.

ASTM E2213-03 is the standard specification for telecommunications and information exchange between roadside and vehicle systems.³ This standard generally specifies MAC and PHY layers for wireless connectivity in the DSRC band of 5.9 GHz. It is an extension to the IEEE 802.11 standard for high-speed mobile environments and is based on the MAC and PHY layer specifications of the IEEE 802.11 and IEEE 802.11a technology standards. It describes communication specifications among roadside and onboard mobile units in the line-of-sight distances of up to 1km. Privacy and authentication procedures have also been incorporated within this standard.

Top Challenges

User-Defined Protocols. While the IEEE VAN standard has been recently released, user-defined protocols are needed to allow researchers and industry work on various applications, prototypes, and products.

Modified 802.11. Vehicular networks demand robust wireless connectivity for high-speed mobile outdoor environments. The original IEEE 802.11 standard does not meet these requirements, and thus, there is a pressing need for a modified version of this standard for VAN applications. The problems of 802.11 mainly include mobility, multi-path propagation due to reflection in non-line-of-sight conditions, RF Doppler effect, and low network bandwidth of 2Mbps.¹⁷ Security challenges such as incorporating authentication features and encryption/decryption methods are also of concern. The IEEE 802.11p technology should be deployed in VAN as complementary technology to WiFi, 3G, and WiMAX to address the issues noted here, and enable V2I and V2V for safety and emergency communications.

Scalability of 802.11p. The current MAC parameters of the IEEE 802.11p protocol are not efficiently configured

for a potential large number of vehicles. The efficiency, performance, and throughput decrease as the number of vehicles increases.⁴⁷ Therefore, centralized or distributed techniques that compute/estimate the number of communicating vehicles in a geographical area should be taken into consideration. Furthermore, in the current 802.11p protocol, the number of collisions dramatically increases as the number of vehicles increases.¹⁰ On the other hand, issues such as packet loss come into the picture as the speed of vehicles increases.³⁵ For all these reasons, advanced techniques should be integrated within the IEEE 802.11p standard to overcome such scalability issues.

Existing Wireless Solutions

Cohda Wireless Ltd, a developer in the area of safe vehicle and connected vehicle designs (www.cohdawireless.com), has addressed the mobility and outdoor Non-Line-Of-Sight (NLOS) issues due to long delay spread and multipath propagation by designing a radio on Wi-Fi chipsets. Particularly, Cohda wireless has implemented the MK2 WAVE-DSRC Radio, which is an IEEE 802.11p-compliant device suitable for V2V and V2I communication in WAVE. At present, Atheros (www.atheros.com) and Broadcom (www.broadcom.com) have, at least partial support for 802.11p. There are other device manufacturers that have developed 802.11p-compliant systems (for example, www.aradasystems.com and www.redpinesignals.com). All these solutions suggest that 802.11p is the front-runner for serious deployment in VAN.

Simultaneously in academia, researchers have devised smart adaptive antennas and cooperative/cognitive radios for wireless connectivity in vehicular networks.⁵³

Security and Privacy of VAN

A number of security mechanisms has been integrated within the IEEE P1609.2 standard,⁴⁶ enabling security and privacy features for vehicle-area-networks. These issues are of significant importance and should be devised before VAN becomes fully operational. Imagine how false or stolen data such as driver behavior, vehicle functional information, environmental hazards, or road condition data could cause

harm if the network is not secured and if the privacy of each individual is not protected. Consider a node (for example, a driver or vehicle) that can insert false information about other drivers and traffic, or the one that can eavesdrop private information and use this information against other users in his or her own favor (for example, to stop or mislead a flow of vehicles).

Another issue in security of VAN is the mobility feature of vehicles, which could easily result in rapid changes in the VAN topology. Thus, security and privacy protocols should be carefully designed to avoid overwhelming the radio link bandwidth with sudden node density fluctuations. In addition, due to having so many participating elements, we open the door for unintentional network congestion, or intentional flooding of the network with junk data that would result in denial of service.⁶ This is critical, particularly for VAN, as attackers may completely bring down vehicular networks this way.

While all the cases here are anti-social behaviors, they are real-life possibilities with devastating results in terms of public safety. Papadimitratos et al.¹⁴ explain how the sweet dream of deploying VANs may turn into a nightmare if security and privacy elements are not carefully embedded. In that case, the disadvantages of deploying vehicular communications in VANs would be more than the benefits.

Many researchers in academia and industry have investigated secure vehicular communications in ITS-VAN.³² Among those are cryptography, public or private keys, and digital signature verification approaches for security and privacy as well as redundant packets delivery for a more reliable communication.³¹ Others have worked on schemes that can be used on top of the IEEE 1609.2 standard for secure messaging protocols in WAVE.⁵⁰

Anomaly detection systems can be employed to minimize the effect of malicious breaches on VAN.^{2,13,43} The main idea is to employ data/packet processing techniques (for example, packet content inspection such as worm detection,^{13,29,40} or machine learning⁵) for such behavioral analysis. Other techniques include continuous monitoring of network flow to identify anomalies

or malicious attempts.⁵² Here, we list a few cases where anomaly detection can be effectively deployed to enhance VAN security or safety:

Driver Profiling: Machine learning and classification techniques are required to profile the driver's behavior.^{5,43} A driver profile could be generated based on the driver's physiological signals (for example, ECG, EEG, EOG) or vehicle information (speed, GPS routing, tire traction and stability) collected from various sensors. For instance, a profiling curve can be constructed based on the frequencies of certain metrics where abnormalities are reflected by any distortions from the normal curve.

Fatigue Detection: In driver fatigue detection systems, a driver behavioral analysis platform can be devised to analyze and differentiate normal vs. abnormal regions representing the alert vs. non-alert status of a driver.⁴³ This platform requires an innovative classifier for detecting driver fatigue by providing a novel profiling curve of the collected driver (or vehicle) behavior.

VAN Communication: All three types of communication in VAN can benefit from devising an anomaly detection system:

- ▶ *V2V:* For security in V2V communication, the network side as well as the client (vehicle) side should be equipped with content inspection or anomaly detection engines to combat intrusions, phishing, spam, and denial-of-service attacks.

- ▶ *V2B:* A profiling and classification system can be integrated within V2B communications effectively. For example, a central monitoring station can assess normalcy of a driver's behavior and diagnose a vehicle's malfunction occurrences. Behavioral analysis can be used to identify a normal region for any subset of parameters of interest.

- ▶ *V2I:* In V2I communications, vehicles receive a large volume of data from route environment (sensor nodes planted on roads, other vehicles, or roadside units).

Thus, the security against undesired or malicious incoming data becomes a challenge. Anomaly detection schemes can analyze data, identify suspicious strings (or even situations), raise alarm and overall protect the vehicle network from possible attacks and failures.

Secure Communication

According to Williamson,⁵² security and privacy in VAN communication should account for features such as message authentication, integrity, accountability and privacy protection. Current research on security in vehicular communication protocols mostly focuses on periodic beaconing, flooding, Geocast and position-based mechanisms.^{21,37,48}

Geocast refers to multi-hop broadcast information dissemination in a large geographically restricted destination region. It is important to secure VAN's geocast against denial-of-service attacks caused by overloading. According to Schoch et al.,³⁷ secure Geocast (where a large number of nodes forward a message), can be achieved by employing probabilistic protocols such as advanced adaptive gossiping techniques along with adaptive load control mechanisms. These techniques probabilistically choose a subset of nodes for message forwarding and dynamically control the load on each node to prevent congestion and overloading. On the other hand, security of VAN can be compromised by attacks that cause jamming where the reception of messages is blocked. Jamming attacks can be overcome by using message loss avoidance techniques such as the one introduced in Schoch.³⁷ In this technique the unreceived messages are detected, stored, and queued for retransmission.

The Secure Vehicular Communication (SeVeCom) project,³⁸ funded and carried out by European organizations, focused on the design and practical implementation aspects of security and privacy in VAN. Digital signatures are known as the underlying basis to support security and anonymity in VAN. SeVeCom made use of customized hardware security modules (HSM), implemented as application-specific integrated circuits (ASIC) both onboard and at the roadside infrastructure to support cryptographic operations. HSM stores and protects private keys for digital signature generation, and handles the key and device management. SeVeCom relies on multiple short-term certified private-private key pairs, known as pseudonyms, rather than traditional long-term private and public keys for

each vehicle. Pseudonym authentication, credential/identity management and revocation of compromised modules are assumed to take place at certification authorities instantiated at the roadside infrastructure.

Top Challenges and Existing Solutions

Adapting to Future Platforms. According to Kargl et al.,²¹ in order to have a compatible architecture that can adapt to the ever-growing future vehicular technologies, integration of the security and privacy features should be based on the hooking concept where interlayer proxies are placed at several points of the communication stack. This way, only these intermediate layers must be configured if the security features are to be migrated to new platforms. The SeVeCom project implemented in-vehicle security by introducing a firewall that controls the data flow to and from the vehicle, and is also devising an intrusion detection system (IDS) that constantly monitors the data flow and detects attacks/anomalies or denies system access in real time.

Secure Beacons. Safety/Secure beaconing in which periodic beacon messages are digitally signed and certified may become a challenge as the security communication will incur an overhead due to signature generation and certificates attached to each packet. The performance of VAN security can be enhanced by utilizing compact certificates, in which not all messages get certificate attachments.²¹ Instead, signatures and certificates are cached, removed in certain cases, or only generated after every few successive beacons. However, context-adaptive message dissemination, gossiping, and data aggregation are also interesting techniques that can be considered for vehicular systems.

Privacy Issues. Privacy protection in VAN mostly deals with providing anonymity for vehicle message transmissions such that vehicle/user's private information, especially location may not be easily traced. SeVeCom has integrated privacy features in VAN by making use of pseudonyms and frequently changing these pseudonyms, making vehicle tracking nontrivial.²¹ Since vehicles may be fully tracked even be-



Integration of security and privacy features should be based on the hooking concept where interlayer proxies are placed at several points of the communication stack.




tween pseudonym changes, challenges lie in devising new mechanisms that support privacy in VAN. Some techniques rely on group signatures where a number of vehicles in near proximity that are traveling with almost the same velocity can be grouped together. In the case of grouping, only one signature will be generated for the whole group, thus enhancing the group member vehicles' anonymity and privacy.³⁶ However, such techniques may not be efficient for actual deployment, and hence other techniques such as hybrid solutions to VAN privacy are required and remain as current ongoing research efforts.

Real-world Simulation. Many works have simulated the performance and security features of VAN by synthetically forming a VAN network topology. Real-world scenarios of a potentially large network of vehicles consisting of hundreds of vehicles in large geographical areas need to be emulated to capture the actual performance of VAN, especially under certain attacks (for example, overloading or jamming), and/or other type of congestions. The work in Haas et al.¹⁵ simulated a relatively large and dense network of vehicles under accident-like scenarios, and reported how VAN would perform in terms of speed of the vehicles, message reception, and so on. Other real-life scenarios should be integrated within the simulations to reflect the actual advantages or disadvantages of various VAN techniques.

Securing Vehicle Access Control and Theft Prevention. Security and privacy of VAN deals with secure and private communication such as preventing unauthorized vehicle access, attacks against in-vehicle control systems, and attacks over diagnostic onboard units and sensors (for example, exploiting tire pressure monitoring). It should also provide anti-theft features for vehicles. Though techniques such as a remote kill switch (that remotely shuts off the engine in case of vehicle theft) have been implemented (www.3built.com), vehicle theft prevention still remains as a security challenge of VAN. Additionally, as there are techniques to duplicate real keys from only an image,²⁵ it is clear that security concerns should be taken more seriously into consideration.

Conclusion

This article provided an insight into future intelligent vehicle area networks. The key elements of VAN were explained and the main challenges as well as ongoing research have been discussed. In particular, intelligent in-vehicle systems, and the main inter-vehicle communication elements, that is, V2V, V2B, and V2I, along with three key IEEE/ASTM standards, was discussed. Research work addressing VAN security and privacy were briefly addressed.

We envision future VAN combining wireless local and wide area network technologies using portable IP-centric devices, sensors, signal processing, and driver behavior analysis techniques. This would ensure reliable and informative communication while vehicles are in motion. Ultimately, the future vehicle area networks would collect driver/car/road data, quickly analyze and share the information to provide a safe, secure, and pleasant driving environment in future networks of smart vehicles. 

References

- Abdalla, G.M.T., Abu-Rgheff, M.A. and Senouci, S.M. Current trends in vehicular ad-hoc networks. In *Proceedings of the IEEE Global Information Infrastructure Symposium*, (2007), 1–7.
- Androulidakis, G., Chatzigiannakis, V. and Papavassiliou, S. Network anomaly detection and classification via opportunistic sampling. *IEEE Network* 23, 1 (Jan.-Feb. 2009), 6–12.
- ASTM International. E2213-03 Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems; <http://www.astm.org>.
- Barth, A. and Franke, U. Where will the oncoming vehicle be the next second? *IEEE Intelligent Vehicles Symposium* (June 2008), 1068–1073.
- Bishop, C.M. *Pattern Recognition and Machine Learning*. Springer, Berlin, 2006.
- Blum, J.J., Neiswender, A. and Eskandarian, A. Denial of service attacks on inter-vehicle communication networks. In *11th IEEE International Conference on Intelligent Transportation Systems* (Oct. 2008), 797–802.
- Chiku, N. et al. A study of lane keep support system based on human driving characteristics. In *Proceedings of the JSAE Annual Spring Congress 19-01* (2001), 1–4.
- Cobb, W. *Recommendation for the Practice of Clinical Neurophysiology*. Elsevier, Amsterdam, 1983.
- Department of Transportation. Saving Lives through Advanced Vehicle Safety Technology; www.its.dot.gov/iv/docs/AR2001.pdf.
- Eichler, S. Performance evaluation of the IEEE 802.11p WAVE communication standard. In *Proceedings of the IEEE Vehicular Technology Conference*, (Oct. 2007), 2199–2203.
- Endo, T. et al. Development of reverse parking assist with automatic steering. In *Proceedings of the 10th ITS World Congress*, Nov. 2003.
- Ergen, S.C., Sangiovanni-Vincentelli, A., Sun, X., Tebano, R., Alalusi, S., Audisio, G. and Sabatini, M. The tire as an intelligent sensor. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 28, 7 (July 2009), 941–955.
- Faezipour, M., Nourani, M. and Panigrahy, R. A hardware platform for efficient worm outbreak detection. *ACM Transactions on Design Automation of Electronic Systems* 14, 4 (Aug. 2009), 49–67.
- Gansen, T., Wischhof, L., Ebner, A. and Paulus, I. Car-2-X challenges—Dreams and nightmares. *Secure Vehicular Communications Workshop: Results and Challenges Ahead*, Feb. 2008.
- Haas, J.J. and Hu, Y.-C. Communication requirements for crash avoidance. In *Proceedings of the 7th ACM International Workshop on Vehicular Ad Hoc Networks* (Sept. 2010).
- Healey, J.A. and Picard, R.W. Detecting stress during real-world driving tasks using physiological sensors. *IEEE Transactions on Intelligent Transportation Systems* 6, 2 (June 2005), 156–166.
- IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (2007); <http://standards.ieee.org/>
- Ishida, S. et al. The method of a driver assistance system and analysis of a driver's behavior. In *Proceedings of the 10th World Congress of ITS*, 2003.
- Jiang, D., Delgrossi, L., Gerla, M. and Jiang, Y. IEEE 802.11p: Towards an international standard for wireless access in vehicular environments. In *Proceedings of the 67th IEEE Vehicular Technology Conference*, (May 2008), 2036–2040.
- Johansson, K.H., Torngrén, M. and Nielsen, L. Vehicle applications of controller area network. Technical Report, Department of Signals, Sensors and Systems, Royal Institute of Technology, Stockholm, Sweden, and Department of Electrical Engineering, Linköping University, Sweden, 2003.
- Kargl, F., Papadimitratos, P., Buttyan, L., Mter, M., Schoch, E., Wiedersheim, B., Thong, T.-V., Calandriello, G., Held, A., Kung, A. and Hubaux, J.P. Secure vehicular communication systems: Implementation, performance, and research challenges. *IEEE Communications Magazine* 46, 11 (Nov. 2008), 110–118.
- Kato, S. Driver assistance with cooperative driving. In *Proceedings of AVEC*, 2004.
- Kitasuka, T., Nakanishi, T. and Fukuda, A. Wireless LAN-based indoor positioning system WIPS and its simulation. In *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing* (2003), 271–275.
- Kubota, S., Okamoto, Y. and Oda, H. Safety driving support system using RFID for prevention of pedestrian-involved accidents. In *Proceedings of the 6th International IEEE Conference on ITS Telecommunication* (June 2006), 226–229.
- Laxton, B., Wang, K. and Savage, S. Reconsidering physical key secrecy: Teleduplication via optical decoding. In *Proceedings of the ACM Conference on Computer and Communications Security* (Oct. 2008), 469–478.
- Lotan, T. and Toledo, T. An in-vehicle data recorder for evaluation of driving behavior and safety. *TRB 2006 Annual Meeting*.
- Motsinger, C. and Hubing, T. A Review of Vehicle-to-Vehicle and Vehicle-to-Infrastructure Initiatives. Technical Report, Clemson University, CVEI-07-003, Oct. 2007.
- National Highway Safety Administration. *USDOT NHTSA Press*, (June 2007).
- Nourani, M. and Katta, P. Bloom filter accelerator for string matching. In *Proceedings of the 16th International Conference on Computer Communications and Networks* (Aug. 2007), 185–190.
- Papadimitratos, P., Buttyan, L., Holzer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A. and Hubaux, J.-P. Secure vehicular communications: Design and architecture. *IEEE Communications* 46, 11, (Nov. 2008), 100–109.
- Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A. and Raya, M. Architecture for secure and private vehicular communications. In *Proceedings of the 7th International Conference on ITS Telecommunications* (June 2007), 1–6.
- Papadimitratos, P., Gligor, V. and Hubaux, J.-P. Securing vehicular communications—assumptions, requirements, and principles. In *Proceedings of the 4th Workshop on Embedded Security in Cars* (Nov. 2006), 5–14.
- Pottie, G.J. and Kaiser, W.J. Wireless integrated network sensors. *Commun. ACM* 43, 5 (May 2000), 51–58.
- Saeed, A., Faezipour, M., Nourani, M. and Tamil, L.S. Plug-and-play sensor node for body area networks. In *Proceedings of the IEEE/ACM Life Science Systems and Applications Workshop*, (Apr. 2009), 104–107.
- Saeed, R.A., Hj Naemat, A.B., Aris, A.B., Khamis, I.M. and Awang, K.B. Evaluation of the IEEE 802.11p-based TDMA MAC method for road side-to-vehicle communications. *International Journal of Network and Mobile Technologies* 1, 2 (Nov. 2010), 81–87.
- Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. and Sezaki, K. CARAVAN: Providing location privacy for VANET. *Embedded Security in Cars*, Nov. 2005; also in *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks* 25, 8 (Oct. 2007), 1569–1589.
- Schoch, E., Bako, B., Dietzel, S. and Kargl, F. Dependable and secure geocast in vehicular networks. *ACM VANET Workshop*, 2010.
- SeVeCom. Secure Vehicular Communications: Security Architecture and Mechanisms for V2V/V2I, Deliverable 2.1 (2007–2008); <http://www.sevecom.org/>
- Sikora, A. Communication and localization for a cooperative safety-system. In *Proceedings of the IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, (Sept. 2007), 682–685.
- Singh, S., Estan, C., Varghese, G. and Savage, S. Automated worm fingerprinting. In *Proceedings of the ACM Symposium on Operating System Design and Implementation* (Dec. 2004), 45–60.
- Sohn, T., Varshavsky, A., LaMarca, A., Chen, M.Y., Choudhury, T., Consolvo, S., Hightower, J., Griswold, W.G. and de Lara, E. Mobility detection using everyday GSM traces. In *Proceedings of the 8th Conference on Ubiquitous Computing* (2006).
- Sun, Q. and Garcia-Molina, H. Using Ad-hoc Inter-Vehicle Networks for Regional Alerts. Technical Report, InfoLab, Stanford University, 2005.
- Takeda, K., Hansen, J.H.L., Erdogan, H. and Abut, H. *In-Vehicle Corpus and Signal Processing for Driver Behavior*. Springer Press, 2009.
- Takei, Y. and Furukawa, Y. Estimate of driver's fatigue through steering motion. In *Proceedings of the IEEE Man and Cybernetics International Conference 2* (2005), 1765–1770.
- Tipping, M.E. Sparse Bayesian learning and the relevance vector machine. *Journal of Machine Learning Research* 1 (2001), 211–244.
- U.S. Department of Transportation. IEEE 1609—Family of Standards for Wireless Access in Vehicular Environments (WAVE), Jan. 2006; <http://www.standards.its.dot.gov/fact-sheet.asp?i=80/>
- Wang, Y., Ahmed, A., Krishnamachari, B. and Psounis, K. IEEE 802.11p Performance Evaluation and Protocol Enhancement. In *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety*, (Sept. 2008), 317–322.
- Weimerskirch, A., Haas, J. J., Hu, Y.-C. and Laberteaux, K.P. Data security in vehicular communication networks. In *VANET Vehicular Applications and Inter-Networking Technologies*. H. Hartenstein and K.P. Laberteaux, Eds. John Wiley & Sons, Ltd., Mar. 2010.
- Weng, T.L. and Gupta, R. ENLS—A Framework for Localization Services for Mobile Computing. University of California, San Diego, Jacobs School of Engineering Research Expo Poster, Feb. 2008.
- Whyte, W. Vehicle security in VII. *Secure Vehicular Communications Workshop: Results and Challenges Ahead*, Feb. 2008.
- Wilcox, J. Microsoft will take Toyota cars to the cloud (Apr. 2011); www.betanews.com/
- Williamson, M.M. Throttling viruses: Restricting propagation to defeat malicious mobile code. In *Proceedings of the 18th Annual IEEE Computer Security Applications Conference* (Dec. 2002), 61–68.
- Xiang, W. A vehicular ultra-wideband channel model for future wireless intra-vehicle communications systems. In *Proceedings of IEEE Vehicular Technology Conference* (Sept.-Oct. 2007), 2159–2163.
- Yamada, M. et al. Study of a road surface condition technique in the human centered ITS view aid system. In *Proceedings of the 9th World Congress of ITS*, 2002.
- Yousefi, S., Mousavi, M.S. and Fathy, M. Vehicular ad-hoc networks (VANETs): Challenges and perspectives. In *Proceedings of the 6th IEEE International Conference on ITS Telecommunication*, (2006), 761–766.
- Zhang, Z. and Zhang, J.S. Driver fatigue detection based intelligent vehicle control. In *Proceedings of the 18th IEEE International Conference on Pattern Recognition* (Washington, DC, 2006), 1262–1265.

Miad Faezipour (mfaezipo@bridgeport.edu) is an assistant professor of computer science and engineering at the University of Bridgeport, CT.

Mehrdad Nourani (nourani@utdallas.edu) is a professor in the Department of Electrical Engineering at the University of Texas at Dallas.

Adnan Saeed (axs055200@utdallas.edu) is a Ph.D. candidate in the Department of Electrical Engineering at the University of Texas at Dallas.

Sateesh Addepalli (sateeshk@cisco.com) is Director of the Advanced Research and Innovation Group at Cisco Systems Inc., San Jose, CA.