Connected car and CO_2 emission overview: solutions, challenges and opportunities

Asmaâ Berdigh*

IA Laboratory – Faculty of Sciences,
Moulay Ismail University,
P.B. 11201 Zitoune Meknès, Morocco
Email: asmaberdigh@gmail.com
*Corresponding author

Kenza Oufaska

TICLab Laboratory,
International University of Rabat,
Parc Technopolis Rabat-Shore,
Rocade Rabat-Salé – 11 100 Sala Al Jadida, Morocco
Email: Kenza.Oufaska@uir.ac.ma

Khalid El Yassini

IA Laboratory – Faculty of Sciences,
Moulay Ismail University,
P.B. 11201 Zitoune Meknès, Morocco
Email: Khalid.ElYassini@gmail.com

Abstract: In this paper, we define the key concepts of IoV as an application of IoT: connected car and an overview of the different communication cases leaded from vehicle to-x namely, vehicle-to-vehicle (V2V), vehicle-to-internet (V2I) and vehicle-to-road infrastructure (V2R). We also identify promising area of research, intra-vehicle connectivity and the wireless technologies likely to be used for building an intra-vehicle wireless sensor networks. This paper highlighted also the most recurrent transport issues and the IoT outcome solutions, there characteristics and challenges, within a focus on the intra-vehicular wireless sensor networks.

Keywords: connected car; IoV; intra-vehicle connectivity; vehicle-to-vehicle; V2V; vehicle-to-internet; V2I; vehicle-to-road infrastructure; V2R; wireless technologies; CO_2 emission.

Reference to this paper should be made as follows: Berdigh, A., Oufaska, K. and El Yassini, K. (2019) 'Connected car and CO_2 emission overview: solutions, challenges and opportunities', *Int. J. Information Privacy, Security and Integrity*, Vol. 4, No. 1, pp.65–78.

Biographical notes: Asmaâ Berdigh a PhD student at the Faculty of Sciences from Mouldy Ismail University, Meknes-Morocco. After holding an engineering degree on embedded systems and industrial computing from National Schools of Applied Sciences (ENSA, Fes) Morocco, she works as a R&D Automotive Engineer.

Kenza Oufaska is an Assistant Professor and Scientific Researcher at Faculty of Computer Sciences and Logistics in the International University of Rabat, Morocco. After holding an MSc in Software Engineering from Faculty of Sciences of Abdelmalek Essaadi University in Tetouan-Morocco, she earned her PhD in Mathematics and Computer Science at Moulay Ismail University in Meknès-Morocco. Her main current activities focus on linear programming and multi-objective optimisation, telecommunications, intelligent systems (smart cities and smart vehicles), logistics engineering, and green logistics with applications in humanitarian logistics.

Khalid El Yassini holds a PhD and MSc in Mathematics (University of Sherbrooke – Canada, 2000 and 1994). Previously, he had a degree in Applied Mathematics (Statistics) at Abdelmalek Essaadi University in Morocco (1991). During his academic career, he has taught in several Canadian and Moroccan institutions such as UdeS, UQAR, St-Boniface University, International University of Rabat or Royal Military Academy. He has taught various courses in mathematics, computer science, operations research and logistics. His current research activities focus on mathematical programming, artificial intelligence, information systems, security in computer networks, telecommunications, intelligent systems, and logistics engineering with applications in hospital field or medication domain. Currently, he is a Professor in the Faculty of Sciences at Moulay Ismail University, Morocco.

This paper is a revised and expanded version of a paper entitled 'Connected car and CO_2 emission overview: solutions, challenges and opportunities' presented at The 1st International Conference on Networking, Information Systems & Security (NISS2018), Tangier, Morocco, 27–28 April 2018.

1 Introduction

The internet of vehicles (IoV) is an internet of things (IoT) application in the intelligent transport system and which has prompted a lot of research. The IoV can be used to collect, transmit, identify, integrate and make use of information from cars. It can get intelligent identification, location, tracking, monitoring and management and is therefore considered to be the most likely to have the greatest industrial potential in the IoT application.

1.1 Internet of the vehicle

The vehicles sales have increased dramatically in recent times around the world and will continue to increase (Alam, 2015), as shown in the Figure 1. Moreover, 90% will be connected, by 2020 (https://www.fool.com/investmg/general/2016/01/18/intemet-of-things-in-2016-6-stats-eve- ryone-should.aspx).

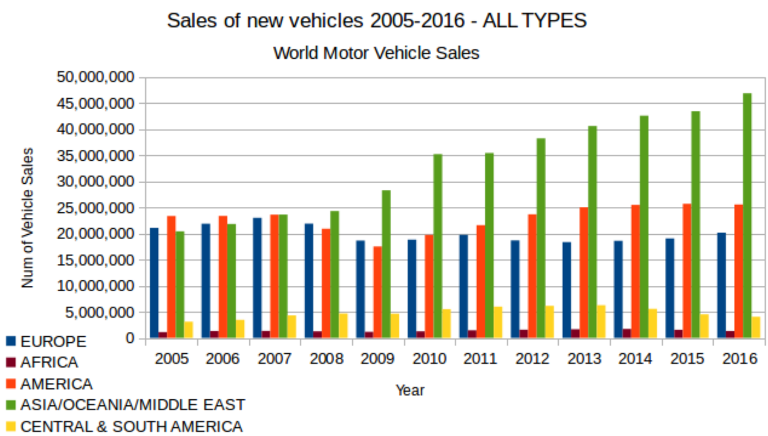
This section provides an overview of to the connected car notion and the in-vehicle networking.

1.2 In-vehicle network

The recent vehicle consists of 50–100 embedded computers (International Organization of Motor Vehicle Manufacturers, 2017), called electronic control units (ECUs), connected to sensors and actuators inside an in-vehicle network. ECUs receive the environment information from sensors and send commands to actuators, to perform their tasks (Kleberger et al., 2011a).

The in-vehicular network is built through different bus system technologies constitute sub-networking interconnected by special gateway ECUs: FlexRay, local interconnect network (LIN) and controller area network (CAN) (Coppola and Morisio, 2016).

Figure 1 Sales of new vehicles 2005–2016 – all types (see online version for colours)



Note: Figure 1 is based on the statistics file *total-sales-2016.xlsx*.

Source: Available at International Organization of Motor Vehicle Manufacturers (2017)

A comparison between the listed above bus, per the main criteria could be found in Table 1.

Table 1 Classic in-vehicle networking bus

Specification	*CAN*	*LIN*	*FlexRay*
Data rate	1 Mbps	20 Kbps	10 Mbps
Physical layer	dual wire	Single wire	dual wire, optical fibre
Architecture	Multi-master, typically 10 to 30 nodes	Single master, typically 2 to 10 slaves	Multi-master, up to 64 nodes
Message transmission type	Asynchronous	Synchronous	Synchronous and Asynchronous
Message identification	Identifier	Identifier	Time slot
Usage	soft real time	Subnets	Hard real time
Latency	Load dependent	Constant	Constant

Note: Table 1 was done based on automotive Trier2 inputs.

Source: Freescale (2013)

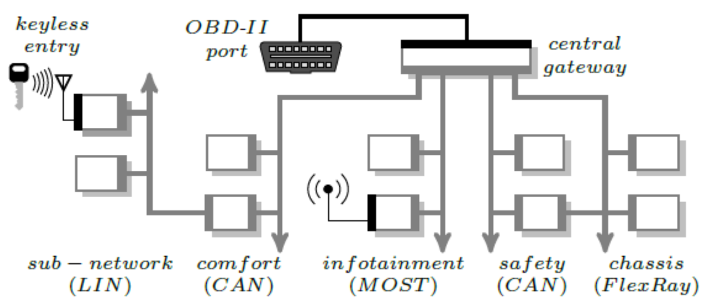
1.2.1 Media oriented system transport

Media oriented system transport (MOST) is a high-speed network classified into Class D networks devoted to multimedia data (Hergenhan and Heiser, 2008), developed in 1998 by MOST cooperation which. This protocol can provide point-to-point data transfer with data rate up to 24.8 Mb/s. MOST defines separately data channels and control channels used to set up the data channels for each link. Once the connection is established, data can flow continuously stream.

1.2.2 IEEE 802.3 Ethernet

IEEE 802.3 Ethernet is a commonly utilised CSMA/CD communication bus protocol due to its low cost, fast speed and high flexibility (IEEE Std. 802.3-201, 2012). Not surprisingly, Ethernet is the technology of choice for much of the Internet and the most popular technology for local area network (LAN) in computer networking. The motivation to implement Ethernet in in-vehicle network is the ever-increasing bandwidth demanded by automotive applications, especially video-based advance drive assistance system (ADAS). The vehicle network should meet different requirements. For instance, the infotainment systems require higher bandwidth, where other systems require fault-tolerant networks. Therefore, a variety of network topologies are combined (Bosch, 2013):

Figure 2 Schematic overview of various in-car networks



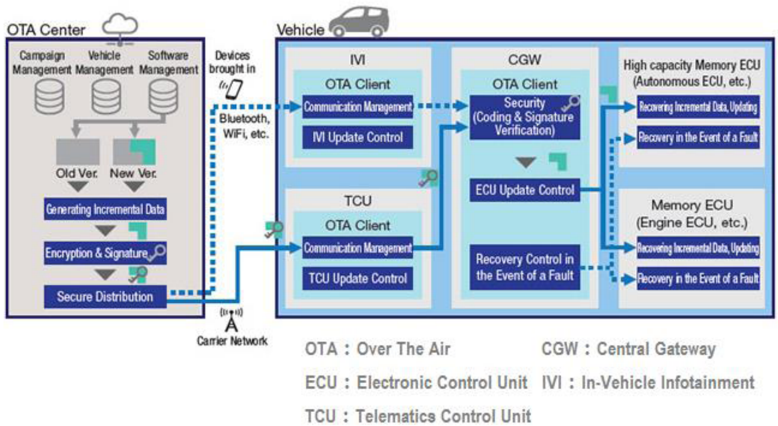
1.3 Connected car

The connected car can be considered as a multi-layered platform or an embedded system equipped with a wireless network gateway connecting the in vehicle network to an external network via over-the air (OTA) technologies and data collection/processing systems.

The connected vehicle allows the exchange of several information between the vehicle and its surroundings using WiFi, Bluetooth and GPS. The connection of the vehicle to the Internet is ensured either by as transmitter/receiver unit integrated with the vehicle itself, or via third-party systems such as smart phones.

Figure 3 illustrates routing of information between a connected vehicle and data centre or OTA centre and point out the steps to control the software updates and assure security of each level (Kleberger et al., 2011a; Sagstetter et al., 2013).

Figure 3 Connected car architecture and information flow (see online version for colours)



A critical challenge for connected cars is the need to prevent damage from cyber-attacks. As in all distributed applications or server-client models, the key to security is an efficient encryption keys management strategy, which ensures the mutual verification of authenticity and protects the communication channels between the centre and the vehicle, as well as between the ECUs of the vehicle.

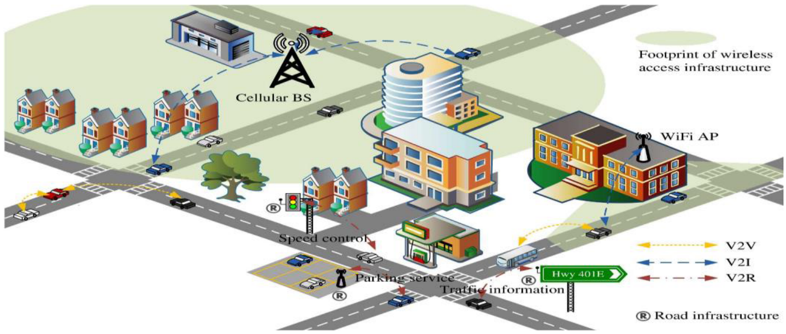
Section 1 gives a state of the art concerning the IoT in transportation as well as definition of serval key concept were defined starting from IoV, in-vehicle network and the car connected. Section 2 will briefly define the most popular architecture inter-network vehicle communication. While Section 3 extends the intra-vehicle connectivity the most technologies used. Section 5 present the discussion of the IoV solutions already adopted and challenges to be overcome.

2 Inter-vehicle communications

As shown in Figure 4, the connected cars have multiple communication possibilities to connect to other vehicles [vehicle-to-vehicle (V2V)] or exchange information with the external environments (vehicle-to-road infrastructure), networks and services [vehicle to internet (V2I)]. These interactions, provide a promising opportunity to address the increasing transportation issues, such as heavy traffic, congestion and vehicle safety.

In this section, we listed succinctly the various types of communications for a connected car detailed in the literature (Qu et al., 2010; Faezipour et al., 2012).

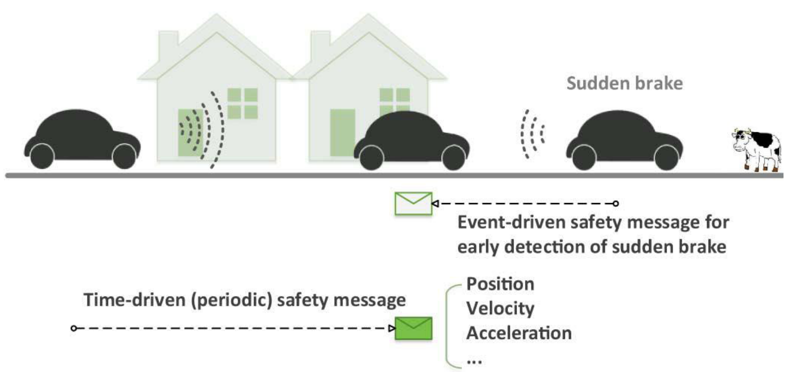
Figure 4 Overview of connected vehicles (see online version for colours)



2.1 Vehicle-to-vehicle

V2V helps improve road safety and improve the efficiency of traffic. In V2V scenario, vehicles exchange wirelessly relevant information to make the driving experience more enjoyable, for example drivers can take steps to reduce the severity or avoid the collision if a sudden brake warning is received earlier. That what affirms the National Highway Traffic Safety Administration (NHTSA, 2017): 'V2V technology has the potential to address approximately 80 percent of multi-vehicle crashes'.

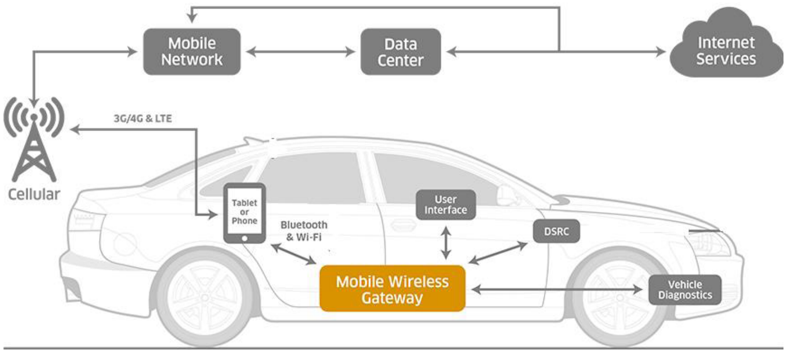
Figure 5 Application of V2V to avoid collision (see online version for colours)



2.2 Vehicle to internet

The connected vehicle shall be able to connect to internet in order to access to different multimedia services. The most common way is using cellular network infrastructures like subscriber identity module (SIM) to allow the vehicle to get connected to the 3G/4G network.

Figure 6 3G vehicle monitoring solution (see online version for colours)



The data centres can query the location using 3G/4G and LTE network, of vehicles at any time, analysis of historical data, video playback, oil and weight loss; this application is illustrated in the in the Figure 6.

2.3 Vehicle-to-road infrastructure

Vehicle-to-road (V2R) connectivity is crucial nowadays for efficient management of intelligent transportation system. The reception of real time road information help in mitigates or avoids the effects of the accidents. Application examples could be a parking lot with infrared devices, WiFi network and parking belts to detect miss parked cars, illustrated in the literature Coppola and Morisio (2016).

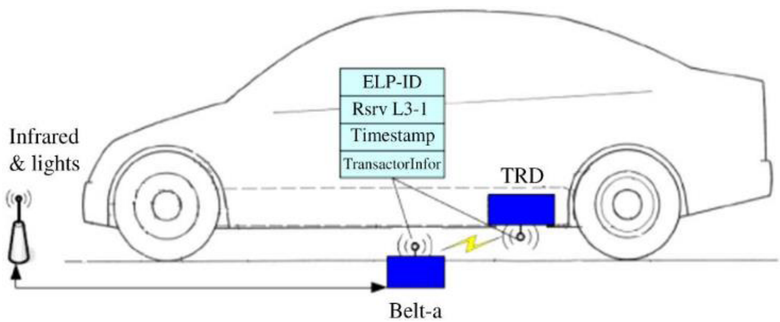
Scenario description

- When a car enters the parking lot and heads to the reserved parking slot, the entrance booth will validate the reservation.
- If the parking spot is validated, a direction-related guidance will be uploaded to the car for finding the reserved spot.
- The road infrastructure engaged: parking belt, lights and infrared device, collaborate to prevent and detect the mismarking. As shown in Figure 7, when the front wheel presses the belt-a, the Bluetooth communication enhanced.
- The belt-a and tamper-resistant device (TRD) illustrated in Figure 4 will validate, as necessary, the reservation confirmation.
- For temporary purpose to validate the parked car the infrared device is used instead of the slot.

For temporary purpose, to validate the parked car the infrared device is used instead of the slot.

The previous section place the IoT concept in automotive context it presented the definition and infrastructure of a connected car and different scenarios of IoT application engaging the inter-vehicular network.

Figure 7 Vacancy of parking slot detections by sensors (see online version for colours)



The idea of Section 3, is to evaluate the possibility of applying the IoT concept inside the Vehicle by transforming the wire intra-vehicular networks to wireless inter-vehicular networks, with the objective to lighten the vehicle weight, reduce the cost of development, harness placements as well as the cost of maintenance and make use of the information technologies advances. So, rethinking the automotive industry to provide a complete intelligent connected vehicle. And therefore, propelling automotive industry toward a new era.

The section start by summarising the most potential wireless communication standards used to perform automotive functions inside a vehicle such as: 'IEEE 802.15.1 – Bluetooth', 'IEEE 802.15.3 – ultra wideband (UWB), high data rate' and 'IEEE 802.15.4 – Ultra wideband (UWB), high data rate' and 'IEEE 802.15.4 – Zigbee, low data rate'. 'Radio-frequency identification (RFID)', 'IEEE 802.11 – WIFI'.

Continuing with the opportunities and proposals for solutions, features and challenges, end up with an advantage example of this approach, reduce the reduction of CO_2 emissions through the weight lighten.

3 Intra-vehicle connectivity

A forecasted increasing number of sensors deployed in cars, up to 200 per vehicle by 2020 (Pinelis, 2013) is required to report time-driven or event-driven messages to the electrical control units (ECU). Consequently, a growing interest is given to the intra-vehicle communication network design (Lu et al., 2014).

We present below the main candidate wireless technologies to build intra-vehicle wireless sensor networks that have been investigated extensively in the literature.

Table 2 The key criteria comparison of the listed above wireless technologies

Standard	*Bluetooth*	*UWB*	*ZigBee*	*WiFi*
IEEE spec.	802.15.1	802.15.3a[1]	802.15.4	802.11b and 802.11g
Frequency band	2.4 GHz	3.1–10.6 GHz	868/915 MHz; 2.4 GHz	2.4 GHz; 5 GHz
Max signal rate	1 Mb/s	110 Mb/s	250 Kb/s	54 Mb/s
Nominal range	10 m	10 m	10 -100 m	100 m
Nominal TX power	0–10 dBm	–41.3 dBm/MHz (–25)	(–25) –0 dBm	15 -20 dBm
Modulation type	GFSK[2]	BPSK, QPSK[3]	BPSK (+ SK), O-QPSK[4]	BPSK, QPSK COFDM, CCK, M-QAM[5]
Max number of cell nodes	8	8	> 65000	2007
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC
Application	Multimedia	Multimedia	Monitoring and control	Multimedia

Notes: 1 – Draft status. 2 – Gaussian frequency SK (GFSK). 3 – Binary/quadrature phase SK (BPSK/QPSK). 4 –Offset-QPSK (O-QPSK). 5 –Orthogonal frequency division multiplexing (OFDM), Coded OFDM (COFDM), Mmultiband OFDM (MB-OFDM), Mary quadrature amplitude modulation (M-QAM) and Complementary code keying (CCK).

3.1 Wireless technologies

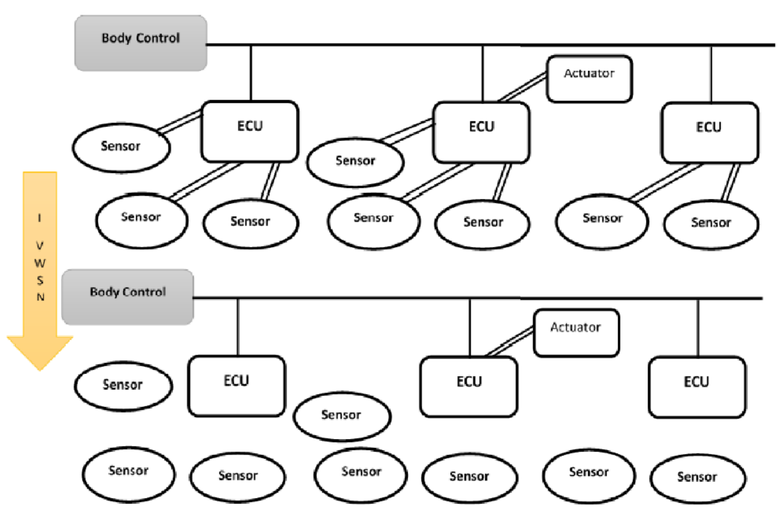
- Bluetooth is a short-range wireless technology based on the IEEE 802.15.1 standard allows a data rate communication up to 3 Mb/s between portable devices (Wang et al., 2013). The Bluetooth devices are common in current vehicles, such as the rear view mirror and Bluetooth headset. However, a Bluetooth network can support just eight active devices, (Gandhi and Jadhav, 2012) and the transmission requires a high-power level, major disadvantage for battery-driven sensors (Qu et al., 2010).
- ZigBee is a short-range wireless technology based on the IEEE 802.15.4 physical radio standard. The ZigBee devices operate in ISM bands at 2.4 GHz and have transmission rates of 250 Kb/s at the 2.4 GHz band with 16 channels, 40 Kb/s at the 915 MHz band with ten channels and 20 Kb/s at the 868 MHz band with 1 channel. Transmission range varies depending on the chosen transmission power (Blasius, 2014), from 10 to 1,600 meters.
- Radio-frequency identification. The feasibility of using the radio-frequency identification (RFID) technology. The rationale of the considered passive RFID solution is that each sensor is equipped with an RFID tag and a reader connected to the ECU, which periodically retrieves the sensed data by sending an energising pulse to each tag (Lu et al., 2014).

- Ultra wideband (UWB) operates on unlicensed frequency band between 3.1 and 10.6 GHz, can support a STA with mobility of 10 kph. It supports low power operation, low power dissipation, robustness for multi-path fading and higher throughput of up to 480 Mbps. Like Bluetooth, it has a transmission range of 10 m. In vehicular ad hoc networks (VANET), it can be used for collision avoidance (Wang et al., 2013).
- Wi-Fi. WLAN is based on the IEEE 802.11 standard family. The most common current versions are 802.11b and 802.11g standards operating in 2.4 GHz bandwidth and capable of up to 54 Mbps or 11 Mbps data speeds, respectively. Recently also some devices supporting forthcoming standard have been published, expected to be able to provide up to hundreds of Mbps data speeds (Gandhi and Jadhav, 2012).

3.2 Solution and opportunities

The evolution of automotive technology, advanced driver assistance systems (ADAS) integrates dedicated functions into more complete systems, require additional components, more sensors and more cameras and more wires and therefore more weight is needed to build larger smarter systems. Cables and other accessories nowadays can add significant weight (up to 50 kg) to the vehicle mass (Qu et al., 2010). Recent advances in wireless sensor communication and networking technologies have paved the way for an intriguing alternative of using cable connection, leading to a significant reduction of the cost and complexity, where ECU and sensors build an intra-vehicle wireless sensor network. As result, more functions could be added to enhance the safety and the intelligence of the vehicle without introducing additional weight, Figure 8.

Figure 8 Intra-vehicular wireless sensor networks (IVWSN) (see online version for colours)



There are advantages to the hybrid wireless concept (Bickel, 2006), such as:

- The weight reduction due to the wires replacement.
- A simpler electrical wiring.
- The easiest maintenance of the electrical submodules.
- A systemic approach to this idea replaced an initial component-level approach.
- Availability and reliability of the off-the-shelf components (ECU, Sensor, actuator) including wireless communication ability.

3.3 Characteristics and challenges

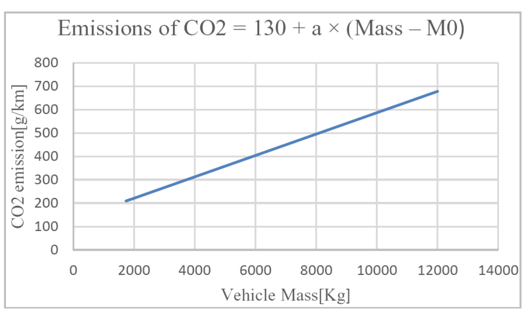
The intra-vehicle wireless sensor networks have specific characteristics:

- Sensors are stationary so that the network topology does not change over time.
- Sensors are typically connected to ECU through one hop, which yields a simple startopology.
- There is no energy constraint for sensors having wired connection to the vehicle power system.

3.4 CO_2 reduction as fundamental driver for weight reduction in automotive

Nowadays, the regulations are forcing OEMs to reduce significantly the car's CO_2. The average emissions, in Europe as an example, of all models sold by an OEM in one year must drop down from about 140 g CO_2 per kilometer to 95 g in 2020 and to 75 g in 2025 and beyond (with some exceptions/adaptations regarding the vehicle class).

Figure 9 Weight impact on CO_2 reduction (see online version for colours)



The precise formula for the value curve is (Visual Media Europe, 2012):

$$\text{Permitted specific emissions of CO2} = 130 \div a \times (M - M0) \tag{1}$$

where

M mass in kg

M0 1,289 kg

a 0.0457 g CO_2/kg.

However, this slope does not reflect the physical correlation between weight and CO_2 emissions, which is at about 0.08 g CO_2 reduction per kilogram saved. Therefore, reducing weight does help reach CO_2 target as shown in the Figure 9.

4 Discussion

The open-up of automotive sector to adopt IoT approach is a promoted area of solutions to the increasing transportation problems such as energy consumption, urban congestion and environmental pollution. Table 3 illustrates the application of IoT cited in some papers for inter-network and intra-network communication solutions provided versus the challenges to overcome.

Table 3 Resume of the IoV applications intra/inter network communication

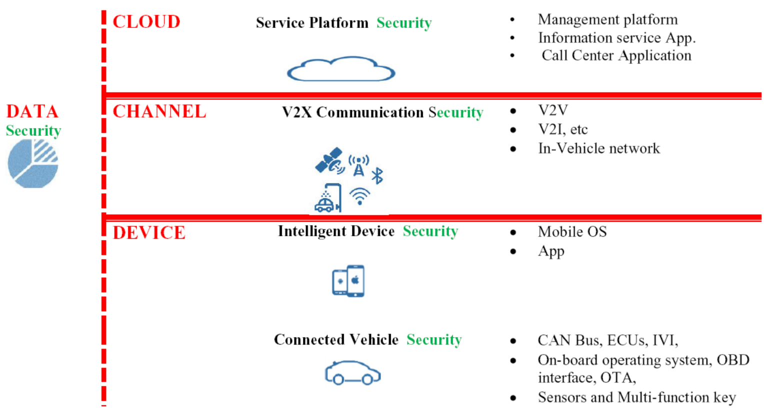
	Papier	*Transport problem*	*IoT application Solution*	*IoT application Challenge*
Inter-network communication	Wang et al. (2013)	Reduce accident and avoid traffic congestion	V2V application	Data security and delay constraints.
	Faezipour et al. (2012)	Increase a traffic safety	V2I application	Bandwidth constraint and data security
	He et al. (2014)	Smarter car and more intelligent systems in the vehicle	V2R application	The Roadside infrastructure involves additional installation costs.
Intra-network	Bickel (2006) and Huo et al. (2015)	Weight maintenance cost reduction and fuel consumption	Intra-vehicular wireless sensor networks	Interferences, malicious attack, real0time requirements

One of the major challenges for developing intelligent and green transportation system, to accelerate the development of connected vehicles is data security, because of the consequence severity of data security indecent. For example, once the traffic management data, or data related to automobile operating, such as brake data, speed, fuel consumption, tire pressure, etc. is falsified or tampered, it will threat the safety of vehicle, passengers and the road management. To assure IoV security we need to fulfil security requirements through the IoV Architecture (Tian, 2017).

5 Conclusions and perspectives

This paper present of the state-of- the-art of IoV. we have discussed the potential challenges of building an intra-vehicle wireless sensor networks and identified the space for future improvement reduce the future car weight, thereby to increase the margin to meet the regulations of CO 2 emission continuously tightened by the governments, In addition, our future work will extend the reliable IoT modeling and simulating a vehicle system (ECU and Sensors eventually actuators) applying the IoT architecture to migrate it from wire communication to a wireless communication system to demonstrate that cable removal is possible while ensuring the same safe functionality.

Figure 10 Security through IoV architecture (see online version for colours)



References

Alam, K.M. (2015) 'Toward social internet of vehicles: concept, architecture and applications', *Fellow*, IEEE, 27 April, Vol. 3, p.343.

Bickel, G.S. (2006) *Inter/Intra-Vehicle Wireless Communication* [online] http://www.cse.wustl.edu/~jain/cse574-06/ftp/vehicular_wireless.pdf (accessed 1 February 2018).

Blasius, J.T. (2014) 'Short-range wireless communications for vehicular ad hoc networking', *Proceedings of the National Conference on Undergraduate Research (NCUR)*, University of Kentucky, Lexington, KY, 3–5 April.

Bosch (2013) *OSI Layers in Automotive Networks*, March, [online] http://www.ieee802.org/1/files/pubhc/docs2013/new-tsn-diarra-osi-layers-in-automotrve-networks-0313-v01 .pdf

Coppola, R. and Morisio, M. (2016) 'Connected Car: Technologies, Issues, Future Trends', *ACM Comput. Surv.*, October, Vol. 49, No. 3, Article 46, 36pp.

Faezipour, M., Nourani, M., Saeed, A. and Addepalli, S. (2012) 'Progress and challenges in intelligent vehicle area networks', *Commun.*, ACM, Vol. 55, No. 2, pp.90–100.

Freescale (2013) *In-Vehicle Networking*, March [online] https://www.nxp.com/docs/en/brochure/BRINVEHICLENET.pdf (accessed 1 November 2018).

Gandhi, A. and Jadhav, B.T. (2012) 'Role of wireless technology for vehicular network', *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 3, No. 4, pp.4823–4828.

He, W., Yan, G. and Xu, L.D. (2014) ''Developing vehicular data cloud services in the IoT environment', *IEEE Transactions on Industrial Informatics*, May, Vol. 10, No. 2, pp.1587–1595.

Hergenhan, A. and Heiser, G. (2008) 'Operating Systems Technology for Converged ECUs', *Proceedings of the 7th Escar Embedded Security in Cars Conference*, November.

Huo, Y., Tu, W., Sheng, Z. and Leung, V.C.M. (2015) 'A survey of in-vehicle communications: requirements, solutions and opportunities in IoT', *IEEE*, Vol. 25, No. 26, p.27.

IEEE Std 802.3-2012 (2012) *IEEE standard for Ethernet*, December, revision to IEEE Std 802.3-2008.

International Organization of Motor Vehicle Manufacturers (2017) *Sales Statistic OICA* [online] http://www.oica.net/cookie-policy/ (accessed 23 December 2017).

Internet of Things in 2016: 6 Stats Everyone Should Know [online] https://www.fool.com/investmg/general/2016/01/18/intemet-of-things-in-2016-6-stats-eve-ryone-should.aspx (accessed 9 November 2017).

Kleberger, P., Javaheri, A., Olovsson, T. and Jonsson, E. (2011a) *A Framework for Assessing the Security of the Connected Car Infrastructure*, 8 November, Vol. 236, ISBN: 978-1-61208-166-3, Chalmers University of Technology.

Kleberger, P., Olovsson, T. and Jonsson, E. (2011b) 'Security aspects of the in-vehicle network in the connected car', in *Intelligent Vehicles Symposium (IV)*, IEEE, p.528533.

Lu, N., Cheng, N., Zhang, N., Shen, X. and Mark, J.W. (2014) 'Connected vehicles: solutions and challenges', *IEEE Internet of Things Journal*, August, Vol. 1, No. 4, pp.289–299.

National Highway Traffic Safety Administration (NHTSA) (2017) [online] https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communications (accessed 24 February 2018).

Pinelis, M. (2013) 'Automotive sensors and electronics: trends and developments in 2013', in *Automot. Sensors Electron. Expo.*, October, Detroit, MI, USA.

Qu, F., Wang, F-Y. and Yang, L. (2010) 'Intelligent transportation spaces: vehicles, traffic, communications and beyond', *IEEE Commun. Mag.*, November, Vol. 48, No. 11, pp.136–142.

Sagstetter, F., Lukasiewycz, M., Steinhorst, S., Wolf, M., Bouard, A., Harris, W.R., Jha, S., Peyrin, T., Poschmann, A. and Chakraborty, S. (2013) 'Security challenges in automotive hardware/software architecture design', in *Proceedings of the Conference on Design, Automation and Test in Europe*, pp.458–463, EDA, Consortium.

Tian, H. (2017) *Introduction of IOV Security*, Security Research Institute, CAICT 2017-1102.

Visual Media Europe (2012) *Lightweight, heavy impact, Advanced Industries*, pp.11–12, February, McKinsey and Company.

Wang, D., O'Keefe, K. and Petovello, M.G. (2013) 'Decentralized cooperative positioning for vehicle-to-vehicle (V2V) application using GPS integrated with UWB range', *Proceedings of the ION 2013 Pacific PNT Meeting*, pp.793–803.