CYBER-PHYSICAL SYSTEMS

Reshaping the Intelligent Transportation Scene: Challenges of an Operational and Safe Internet of Vehicles

Christos Alexakos, Industrial Systems Institute/ATHENA Research Center

Konstantinos Votis and Dimitrios Tzovaras, Centre for Research and Technology-Hellas

Dimitrios Serpanos, University of Patras and CTI DIOPHANTUS

In the emerging era of transportation, the Internet of Vehicles envisions a large ecosystem where vehicles, traffic infrastructure, smart city sensors, and citizens will interoperate, providing safe and fast transportation services. How close are we to realizing this concept?

Digital Object Identifier 10.1109/MC.2021.3125075
Date of current version: 12 January 2022

Following the Internet of Things (IoT) paradigm, where devices sense and actuate in a collaborative environment, the Internet of Vehicles (IoV) envisions the interconnection and cooperation of vehicles, drivers, pedestrians, and smart city infrastructures to ensure the smooth, fast, and safe transportation of citizens to both urban and rural areas. To realize this vision of the IoV, several challenges must be addressed for various components of this complex ecosystem, such as in networking, interoperability, cybersecurity, data privacy, and energy efficiency as well as in applications and services provided by infrastructure systems or mobile devices.[1] We identify major challenges toward making the concept of the IoV a reality in the near future.

0018-9162/22©2022IEEE

EDITOR DIMITRIOS SERPANOS
CTI DIOPHANTUS and University of Patras; serpanos@computer.org

TOWARD AN OPERATIONAL IOV

The IoV (Figure 1) is a system of systems that includes cyberphysical systems, such as autonomous vehicles, smart traffic lights, and a variety of sensors and actuators that interact with the physical environment to collect and share information. A basic operation of an IoV is the exchange of information, even when this information is generated by heterogeneous systems. The problem of interoperability is common in such complex ecosystems; in the IoV, it is crucial. If a vehicle does not understand the messages coming from a parking lot sensor, it cannot proceed to it.

In this direction, a first step has been made with the standardization of vehicle-to-everything (V2X) communications through amendment IEEE 802.11p, which is based on wireless local area networks and the 3G Partnership Project (3GPP), a cellular communications framework.[2] Both 802.11p and 3GPP are adequate for exchanging information between two vehicles as well as between vehicles and the traffic infrastructure such as smart traffic lights.

Yet, the interoperability problem exists for other systems such as IoT sensors. Approaches that introduce integration middleware that organizes information in understandable semantics and formats for the message receiver can be applied, but these solutions require manual effort, and they are specific to the involved systems, rather than generally applied solutions. This indicates the need for new standards in information representation and exchange among all types of IoV components in the coming years.

An operational IoV mandates fast and reliable information exchange among its components. An autonomous vehicle must continuously send and receive data to and from other vehicles, roadside units, or pedestrians, to establish a complete perception of the environment. Its sensors "sense" nearby objects, but the combination of information received through other sources will expand its perception for the environment to a wider geographical range. The requirement for efficient and stable communications becomes more challenging when we consider the physical dimensions of the problem; the vehicles are moving, often fast, inside a city and possibly in the country, where the network infrastructure is inefficient. Furthermore, existing systems that participate in the IoV already have their own communication modules. Smart lights may use the V2X protocol, IoT sensors may use the low-power wide area network or another low-power long-range network, and pedestrians' smart phones have 4G or Wi-Fi connectivity.

The problem of communications in the IoV has a long list of issues to address, from physical barriers to the integration of different communication protocols. Research to overcome these challenges is pivoting in several directions, including the development of wireless networks capable of transferring large amount data fast even in mobile nodes, the minimization of exchanged data to the necessary information latency, and data traffic congestion. The new era of networking introduces 5G and other future cellular networks, which are capable of facing some networking challenges, but they also have their drawbacks.

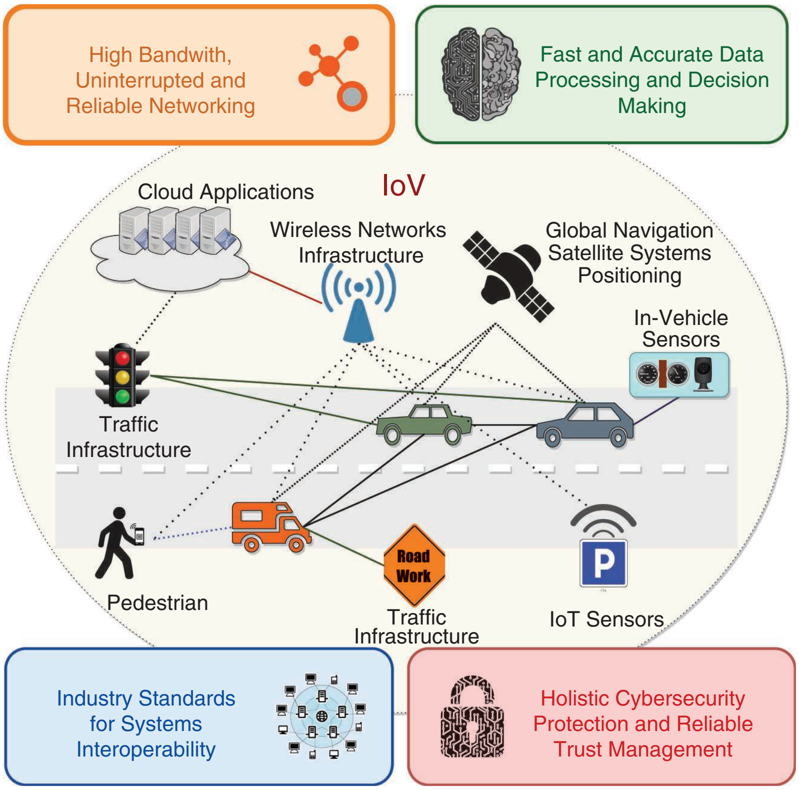
High Bandwith, Uninterrupted and Reliable Networking
Fast and Accurate Data Processing and Decision Making
IoV
Cloud Applications
Wireless Networks Infrastructure
Global Navigation Satellite Systems Positioning
In-Vehicle Sensors
Traffic Infrastructure
Pedestrian
Road Work
Traffic Infrastructure
P
IoT Sensors
Industry Standards for Systems Interoperability
Holistic Cybersecurity Protection and Reliable Trust Management

FIGURE 1. The IoV is a system of systems.

Another point of networking optimization is establishing direct high-bandwidth connections when possible. If one manages to transfer data between two nearby vehicles with a direct link instead of having data travel through a cellular network, the network performance will be increased significantly. However, this requires fast connection establishment and a tolerance of physical barriers that may obstruct communication. Vehicular ad hoc networks focus on this, borrowing principles of mobile ad hoc networks. In a different direction, the minimization of transferred data is an open research field with many opportunities. Even for IoT ecosystems, the need for smaller amounts of transmitted data leads to several approaches such as the use of compression or transmission of differential data. On the other hand, new, more sophisticated, systems embedded in vehicles or other nodes will utilize intelligent algorithms that are capable of isolating the information-valued data for transmission.

The IoV is not only a network of systems but also an ecosystem providing services to citizens. The most important service is safe transportation from one place to another, with an autonomous vehicle, a private connected vehicle, or even on foot. To achieve this, all of the IoV systems are continuously processing data, evaluating the environment, and making decisions. For example, an autonomous vehicle must decide when to stop and start, where to turn, and when to accelerate or brake. Artificial intelligence (AI) plays a lead role in this process. Even today, vehicles are empowered with units that execute algorithms for detecting objects in a camera stream, reading signs, or even deciding to brake to avoid an accident. In an IoV ecosystem, the information used by a vehicle to make a decision originates from several sources inside and outside the vehicle. Larger amounts of data require more resources for processing when we use high-end AI technologies like deep learning.[3] A response to this challenge comes from the edge computing paradigm. Increasingly, more systems intelligence is moving closer to the user and, in the case of the IoV, closer to its crucial components: the vehicles and the roadside systems. The next generation of connected vehicles, autonomous or not, will include systems with thousands of GPUs, increasing the performance of decision algorithms. The current challenge is the optimization of the accuracy of these algorithms, ensuring the provision of high-quality services.

SAFETY AND SECURITY

The digitization of transportation services and the realization of the IoV concept introduce a major concern: how one protects the IoV from malicious cyberattacks and how these attacks may affect citizens' safety. Analogously to IoT environments, the IoV is vulnerable to cyberattacks that may result in fatal accidents. Until now, cyberattacks against connected vehicles resulted in nonlethal incidents such as stopping or locking a car, mainly through attacks against the infotainment system.[4] But these attacks were against individual vehicles. The protection of an IoV system is complex because of the heterogeneity of connected systems, which complicates the work of cybersecurity experts.[5]

Worldwide, international or national cybersecurity agencies are announcing updated information on the identification and categorization of potential attacks on autonomous and connected vehicles, but significantly more work needs to be done for the IoV. The IoV must be protected as a critical infrastructure. Importantly, the IoV is composed of several systems that interoperate closely, and each one of them is a potential target that may compromise the whole network. Thus, cybersecurity solutions must be holistic, and they must cover all layers of the IoV, from communications to the protection of software that is used inside or outside the vehicles. Although the current state-of-the-art cybersecurity solutions make it feasible to construct a protection shield on most IoV components, several aspects still need to be explored.

In most cases of cyberattacks against the IoV, a crucial part is rapid detection and response. If an attacker can manipulate data from the sensors of a vehicle or change the color of a traffic light, an accident may happen in seconds. Cybersecurity solutions must be able to detect this abnormality and respond within a very tight time window. Prominent approaches are oriented to bring the detection and the response inside the IoV's components, either by installing embedded systems that increase security or by integrating detection and response methods in the intelligent systems already installed. For example, a detector for attacking the camera feed can be integrated in the vehicle's main computational unit along with the object detection algorithm. Since the IoV is a dynamic ecosystem, new components—vehicles, sensors or actuators—are continuously connected to it. This raises the problem of trust and authentication of the connected components. Which of the new components can be trusted? How will one know that it is not a malicious system trying to connect to the IoV ecosystem? Proposals based on a Secure Sockets Layer certificate exchange and the use of blockchain technology provide some solutions, but their applicability in a large and complex ecosystem is still a big challenge as most of them have been tested in small pilots or simulation environments.

The IoV is an emerging concept for realistic transportation ecosystems that has led to pilot designs and implementations toward operational maturity. It poses several critical questions and challenges, especially in communications, safety, and cybersecurity. Importantly, an efficient and effective IoV operation involves several stakeholders, from public administration to citizens and from automotive manufacturers to standards bodies, who need to work collectively to address the increasing challenges and enable innovation for the required new services and products. ◼

REFERENCES

1. 1. J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, 2017, doi: 10.1109/JIOT.2017.2690902.
2. V. Vukadinovic et al., "3GPP C-V2X and IEEE 802.11 p for vehicle-to-vehicle communications in highway platooning scenarios," *Ad Hoc Netw.*, vol. 74, pp. 17–29, May 2018, doi: 10.1016/j.adhoc.2018.03.004.
3. H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, 2020, doi: 10.1109/JPROC.2019.2961937.
4. S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Anal. Prevention*, vol. 148, p. 105837, Dec. 2020, doi: 10.1016/j.aap.2020.105837.
5. J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, p. 101823, July 2019, doi: 10.1016/j.adhoc.2018.12.006.

CHRISTOS ALEXAKOS is an associate researcher at the Industrial Systems Institute of ATHENA Research Center, Patras, 26504, Greece. He is a Member of IEEE. Contact him at alexakos@isi.gr.

KONSTANTINOS VOTIS is a senior researcher at the Information Technologies Institute of the Centre for Research and Technology-Hellas, Thermi—Thessaloniki, 57001, Greece. Contact him at kvotis@iti.gr.

DIMITRIOS TZOVARAS is a senior researcher at the Centre for Research and Technology-Hellas, Thermi—Thessaloniki, 57001, Greece. He is a Senior Member of IEEE. Contact him at Dimitrios.Tzovaras@iti.gr.

DIMITRIOS SERPANOS is president of the Computer Technology Institute and Press "Diophantus" and a professor at the University of Patras, Patras, 26504, Greece. He is a Senior Member of IEEE. Contact him at serpanos@computer.org.

Rejuvenating Binary Executables • Visual Privacy Protection • Communications Jamming
IEEE SECURITY & PRIVACY
Building Dependability, Reliability, and Trust
SOFTWARE EVERYWHERE
January/February 2016 Vol. 14, No. 1
Policing Privacy • Dynamic Cloud Certification • Security for High-Risk Users
IEEE SECURITY & PRIVACY
IEEE Symposium on Security and Privacy
March/April 2016 Vol. 14, No. 2
Smart TVs • Code Obfuscation • The Future of Trust
IEEE SECURITY & PRIVACY
ECONOMICS OF CYBERSECURITY PART 2
May/June 2016 Vol. 14, No. 3
S & P

IEEE Security & Privacy **magazine provides articles with both a practical and research bent by the top thinkers in the field.**

- stay current on the latest security tools and theories and gain invaluable practical and research knowledge,
- learn more about the latest techniques and cutting-edge technology, and
- discover case studies, tutorials, columns, and in-depth interviews and podcasts for the information security industry.

computer.org/security

IEEE COMPUTER SOCIETY IEEE

Digital Object Identifier 10.1109/MC.2021.3134344