Vehicles as Connected Resources: Opportunities and Challenges

Soumya Kanti Datta, Jérôme Härri, Christian Bonnet, Rui Pedro Ferreira Da Costa
EURECOM
450 route des Chappes,
06904 Sophia Antipolis, France
E-mails: {dattas, haerri, bonnet, ferreira}@eurecom.fr

***Abstract*—With the introduction of smartphones, cloud & edge computing and mobile Internet, the automotive ecosystem is shifting towards the Internet of Vehicle (IoV). This paper looks at this evolution leading to IoV and identifies related research and engineering challenges including (i) co-existence of cloud, edge computing and data caching strategies at the edge, (ii) integration of data processing and management as IoV services and (iii) seamless interoperability among vehicular sensors, computing platforms and consumer devices. To address these challenges, we present an IoT architecture, which considers vehicles as IoT resources and provides (i) mechanisms to integrate them in an IoV ecosystem and (ii) seamless interoperation among components (e.g. vehicular sensors, computational platform and consumers). The functional elements and operational stages of the architecture also assist in maintaining interoperability among the components.**

I. Introduction

The consumer expectations of the automotive industry have undergone significant change during the last decade. The factors prompting the evolution include mobile Internet, smartphone, powerful On Board Units (OBU) and V2X communications. In parallel, the smart city initiatives are deploying infrastructure to provide better road safety and co-operative mobility management while reducing the effect on environment. According to NTT[1], it is evident that the Auto 1.0 and Auto 2.0 ecosystems are not able to meet the smart city requirements due to the absence of powerful OBUs, V2X hardware, proper standards etc. The automotive industry is responding to the evolution with Auto 3.0. Here the focus is shifting towards (i) supporting intelligent transportation system (ITS) through V2X communications, (ii) exposing vehicular resources through web interfaces for data collection, processing, and storage and (iii) seamless communication and information exchange among vehicular gateways, edge servers, cloud systems and consumer resources.

The Auto 3.0 ecosystem enables automatic vehicle information discovery and exchange with a computing systems and other vehicles. The enhanced access and core networking technologies coupled with computation on vehicular sensor data are the stepping stone for vehicles to be a part of the Internet of Things (IoT) ecosystem. Thus vehicles are considered as a resource [1] for IoT systems. An advantage of this philosophy is that the large variety of vehicular sensor data can now be used for pollution monitoring, traffic flow management and road intersection management, which are essential for smart city initiatives. The expanded IoT ecosystem integrates vehicular data with components from ITS, edge & cloud computing and big data paving way for Internet of Vehicles (IoV). The most important goal of IoV is to enable seamless interoperation exchange among consumer smart devices, vehicular things and external computational platforms (edge and cloud servers). At the same time, it aims to improve the computability, extensibility and sustainability of complex network systems and vehicular information flow. The goal is to reach a collaborative awareness and cognition among consumers, vehicles, IoT resources and computing platforms. Our approach is complementary to [13] as it aims at integrating IoT mechanisms such those described in the special issue in a vehicular context.

This paper aims to study the IoV ecosystem and its current landscape. We identify the research and engineering challenges related to Auto 3.0 and IoV. Our research contributions are - (i) presentation of a data driven IoT architecture that addresses the identified challenges and enables seamless interoperability among consumers, vehicles and computing platforms leading to creation of an IoV ecosystem, (ii) describing a framework (that follows the architecture) and its operational phases to create IoV applications and (iii) deployment details of the framework that advocates for a distributed approach through coexistence of edge and cloud computing platforms.

II. IoV Landscape

A. IoV Use Cases

Despite its current deployment, the success of IoT in future Smart Cities is pledged by the Industry strong tendency to create data silos and individual standards. Integrating vehicles in the IoV ecosystem will require to break these silos in order to provide critical use cases for road automation, such as *rapid detection of road users*, *cooperative contextual map exchanges*, or even *decentralized traffic management*.

Due to the short notice capabilities, autonomous vehicles will not be able to rely only on their own internal sensors, detectors and maps. Vulnerable Road Users (VRU) detected by either another car, or available as a IoT service should be made available to them. Similarly, maps need to be constantly

[1] http://www.ntti3.com/wp-content/uploads/Automotive_as_a_Digital_Business_V1.03-1.pdf

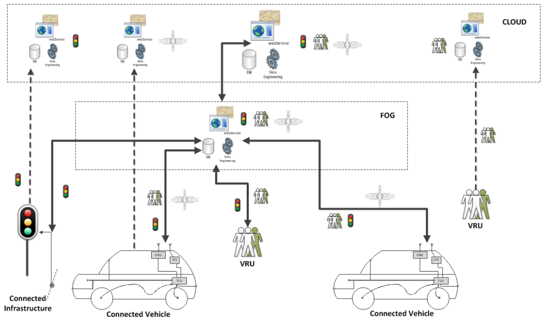


Fig. 1. IoV Use Cases - Data Silos (dash) vs. IoV architecture (pull lines)

enriched with contextual information, which will be observed by other cars or connected infrastructures (road closing, obstacles, traffic). And if these information are further away than the communication range of the V2X technology, autonomous vehicles will need to obtain them from the Cloud via LTE (mobile communication in general).

The key to this success is a rapid data exchange and local data processing for a quick and efficient IoV service. For example, Fig. 1 illustrates the three uses cases, and schematizes their data requirements. VRU, traffic management status (pollution, noise, traffic lights) and navigation maps are all reachable individually by IoT Services (dash line on Fig. 1). However, future autonomous vehicles will require to have access to all of these services, extremely fast and only in their local scopes. Accordingly, VRUs, maps and traffic lights must be locally processed by an IoT gateway located in edge servers (full line in Fig. 1), so that such data is available to all vehicles at very low delay.

A unified architecture is therefore required. As illustrated on Fig. 1, various architectures are present: IoT for the different silos and the Cloud layer, Fog computing at the edge and ITS for the vehicular communications. For information to flow and be correctly interpreted, a unified IoT and ITS architecture is required.

B. *Research and Engineering Challenges*

The envisioned IoV ecosystems are posing several novel research and engineering challenges. We outline a non-exhaustive list below.

- **Seamless Interoperability Support -** The IoV ecosystem is plagued with heterogeneity, individualized development frameworks, data silos and lack of standards. The vehicular sensors (i) generate multi-modal data, (ii) support different encoding format, (iii) belong to heterogeneous domains and (iv) communicate using different radios and protocols. This highlights the heterogeneity at the vehicular resource level. Another aspect is the data representation which affects uniform treatment of data across generic platforms. As there is no standard vocabulary for this, it inevitably leads to platform specific implementation and data silos.
- **Information-Centric Mobile Networks Integration -** Current vehicular networks mostly utilize IPv6 which (i) does not support mobility natively and (ii) is host centric not data centric. But with IoV, communication and networks are becoming enablers for a must larger ecosystem where data processing, management, storage strategies and data dissemination receive more importance. In essence, we need data centric and network independent approach in IoV. Named Data Networking (NDN) is one of the avenues that can mitigate the challenge. But integrating and operating the NDN software stack with rest of the IoV architecture is a massive challenge.
- **Mobile Edge Computing (MEC) Integration -** Co-existence of edge and cloud computing platforms are crucial for offering real time services in IoV. Complete dependency on cloud creates challenges in providing real time services (e.g. autonomous driving scenarios). We must examine mechanisms to operate IoV services from the edge servers (e.g. road side units, vehicular gateways) which complement the capabilities of cloud systems. Another aspect is to study the mechanisms for data caching at the edge servers for IoV applications. This can potentially save network bandwidth, reduce latency and increase quality of service.
- **IoV Best Practice -** IoV being a multi-disciplinary ecosystem, it becomes a huge challenge for the developers to engineer consumer applications. With no widely followed guidelines, such best practices will ease the development time, maintenance and update cycle.

III. State-of-the-Art

This section highlights current landscapes and points out their limitations.

A. *Management of connected vehicles*

Automatic management of connected vehicles and their resources via an edge or a cloud server are important for resource discovery and application development. The authors of [10] proposed a smart vehicle management system that utilizes gateway, hand-set and vehicle management program. In our previous work [4], we have analyzed how to utilize the Open Mobile Alliance (OMA) Lightweight Machine-to-Machine (M2M) Technical Specifications for management of connected vehicles. The main contribution of the paper is in integrating the OMA LwM2M in a MEC platform. Due to the proximity of edge server to vehicles, real time IoV services can be supported. It can also be extended to a cloud platform to manage city traffic in a low cost and scalable way.

B. *Cloud computing and ITS*

The authors of [8] describe an Intersection Control Service (ICS) for urban traffic control. The described ITS framework is cloud assisted. Their main contribution is to describe the interplay of ITS services with cloud that vehicles as cloud services. Vehicle discovery and interaction are also aided by the cloud platform. Each road intersection is managed by an ICS deployed in a RSU. The next level in the hierarchy includes an Area Management Service (AMS) that manages the road network topology and manage traffic on a macro scale. But there is no information about the latency of the application and how much time does it take for the complete operation. The real time aspects of cloud computing enabled vehicular networks are addressed in [14]. It describes a three-tier architecture dealing with device level, communication level and service level. The device level responds to several consumer centric requirements for Auto 3.0. More sensors are being integrated inside the vehicles to monitor driver and passenger health. These devices can form a body area sensor network and exchange information among them. The communication level deals with the communication networks while the service level deploys the core algorithms for ITS (traffic monitoring, pollution, infotainment).

C. Vehicular cloud

Vehicular clouds are explored in [9] where cloud computing services are hosted in vehicles having sufficient resources. This transforms connected vehicles into mobile cloud servers. This work allows vehicles to search for such vehicular clouds, their capabilities and services. The RSUs are utilized as directories by the underlying system. The vehicles offering cloud services must register themselves in the RSUs. This is similar to directory based discovery supported by CoAP. The paper [6] identified two research challenges: (i) urban surveillance service in the vehicular cloud, (ii) vehicular traffic management. To address the evolving vehicular scenarios in a generic way, the vehicular cloud integrates traditional RSUs with microscale data centers. They employ SDN providing deeper granularity in dynamic instantiation, replication and migration of IoV services among them.

D. Security and privacy aspects

Security, privacy and trust increasingly play an important role behind consumer adoption of IoV applications and services. The attack scenarios include sybil attack, GPS detection, masquearading attack, wormhole attack and routing attack. The work also analyses security requirements and countermeasures to the mentioned attacks. In [15], the security issues (namely identity, authentication and integrity) of the vehicles in IoV are investigated. Trusted cryptography module (TCM) is used in this context. A classical attack scenario is denial of service (DoS). Its detection has been discussed in [11] assuming the vehicles are connected to Wi-Fi to access the Internet. DoS attack behavior, its detection algorithm and simulation result validating the approach are presented.

E. Limitations & Challenges

We observe several limitations in the current literature.

- **Lack of data-oriented networking -** Our study reveals that the data driven approach for the IoV is not investigated. The focus of related works is highly on infrastructure, communication technologies, networks and protocols. But these factor are actually enablers of a much larger ecosystem where vehicular and other sensor data and their interpretation play a significant role.
- **Lack of Edge computing support -** Cloud computing platforms cannot support real time IoV applications and services as identified in [4]. MEC is crucial for autonomous vehicles.
- **Lack of Cloud interoperability -** Interoperation of vehicular cloud systems with external cloud platforms are not investigated. The vehicular cloud could also be considered at edge servers which can coexist with data centers enabling robust and scalable IoV ecosystem.
- **Lack of data interoperability -** among the IoV ecosystem components with IoT is not studied in-depth. As mentioned previously, IoV aims to provide seamless interoperability among consumers, vehicles and things. Bridging the interoperability is of utmost importance for the ecosystem to sustain in the longer term.
- **Lack of Best Practice -** Majority of the current approaches do not provide any best-effort guidelines to ease IoV applications development.

IV. IoT Architecture and Components

This section concentrates on an IoT architecture (shown in Fig. 2) to address the challenges and limitations paving the way for IoV. Interactions between the proposed architecture and standard ETSI-ITS architecture is also presented to highlight its interoperability.

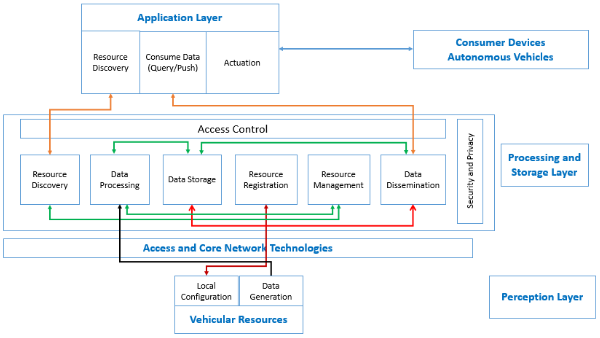


Fig. 2. Functional elements of the IoT architecture enabling IoV

A. Perception layer

The perception layer of the architecture is mainly composed of on-board vehicular resources (sensors, actuators) and smartphone sensors. To integrate these resources into the architecture, the data generated by the resources must be communicated to a computing platform and their configuration must be managed automatically. The inherent challenge is to manage the multi-modality and heterogeneity of the resources. To settle that and maintain interoperability, the architecture utilizes Sensor Markup Language (SenML). With this, additional information (e.g. unit, timestamp, type, name, ID) can be added to the sensor measurement creating a metadata. It eases the data processing at a later stage and can be encoded using JSON, XML, CBOR or EXI.

Description of the vehicular resources is necessary too. We utilize semantic based descriptions [3] that allow the resources to be described in terms of events, properties and actions. This added granularity allows a higher layer application to easily discover the resources through a semantic search engine and understand the capabilities of the resources from their descriptions. They are encoded using JSON-LD. The description is an enabler for registration, resource discovery and management for the processing and storage layer.

Utilizing JSON and JSON-LD (which is basically serialization of Resource Description Framework (RDF) using JSON) maintains interoperability at perception layer. Each vehicle must have the software modules to create and exchange SenML metadata and JSON-LD based descriptions. These capabilities can be integrated into an on board unit (OBU) or a vehicular gateway.

B. Processing and storage layer

This layer houses several functions that are common and necessary to accomplish any IoT and IoV scenarios. Thus they are called common service functions (CSFs) and include - (i) resource registration, (ii) resource discovery, (iii) data management and repository, (iv) data processing through semantic reasoning, (v) security, (vi) access control, (vii) push notification and (viii) resource management. The incoming raw metadata from the perception layer undergoes transformation in this layer and a high level intelligence is derived. This intelligence can be perceived by consumers, vehicles or things participating in an IoV ecosystem. The elements of this layer and their functions are described below. The CSFs are developed using RESTful web services and exposed through web APIs. The reason behind that is the RESTless philosophy is built on keeping sessions for data transfer between a client-server. Standard Development Organizations (SDOs) like W3C and oneM2M [12] recommend using RESTful interactions for IoT.

- Resource registration: The vehicular resources must register themselves into the resource registration element. It operates with a local storage to house the resource descriptions. It is developed using API first approach and provides an API to extract the resource description originating from a vehicle.
- Resource management: Automatic management of vehicular resources are done through this module. It is based on Open Mobile Alliance Lightweight M2M Technical Specifications and details of its implementation has been presented in [2].
- Resource discovery: This CSF allows searching for necessary resources - (i) from which sensor metadata will be collected, and/or (ii) actuation commands will be disseminated. The discovery framework allows consumers or higher layer applications to search for resources using a combination of keywords, attributes and location [5]. Following the discovery procedure, a list of URIs of discovered resources and their descriptions are returned to the requester.
- Data processing: This is the backbone of this layer since the architecture is advocating for a data driven IoV ecosystem. The main challenges to develop a uniform data processing mechanism are the heterogeneity in data and different vocabulary used to represent the data. Semantic web technologies can address them effectively and can transform the raw sensor metadata into high level intelligence. This transformation takes place through several steps. Firstly, the metadata represented in SenML must be converted into RDF. In the second step, semantic rules associated with the domain of operation of the sensor are applied derive a new domain concept.The third step employs domain ontology to classify the new domain concept. The final step applies semantic reasoning (another CSF) and executes SPARQL queries to produce high level intelligence and some suggestions to for actuation based on the scenario. For example, if the data processing mechanism determines there is fog in the driving environment of an autonomous vehicle, then the suggestions will be - (i) reducing the speed of the vehicle and (ii) turning on fog lamps. This is accomplished using Machine-to-Machine Measurement (M3) Framework [7].
- Data management and repository: This module is responsible for local storage and management of high level intelligence and suggestions generated by the data processing CSF. If Named Data Networking (NDN) is utilized for dissemination of the intelligence, then it is converted into appropriate data following NDN naming conventions. Otherwise for HTTP or CoAP based push notifications (another CSF) can also be issued by this module.
- Access control & security: Out of scope of this work, due to the lack of space.

The CSFs of the layer can be deployed at a cloud system as done in the state-of-the-art. But we advocate for distributing the CSFs into both edge servers and cloud platforms. The resource registration, management and discovery services are not latency sensitive and hence can be housed in the cloud. Real time IoV applications will depend on the data processing, high level intelligence and suggestions which must be operated from the edge of communication networks. This coexistence of edge and cloud promotes a distributed architecture, robustness and scalability. This in turn decouples the dependency of the architecture from any specific infrastructure, instead keeps the data driven approach.

C. Application layer

The application logic of the IoV applications run in this layer. This is interfacing directly with consumer of the IoV applications like end users, autonomous vehicles, insurance providers etc. The developers should utilize the open APIs provided by the processing and storage layer to access the CSFs of the architecture over RESTful interactions. We depict the steps to be followed by application developers in Fig. 3.

As seen from Fig. 3, the vehicular sensors, actuators and tag (commonly called resources) must be discovered at first. We assume that the resource configuration, registration and management are already provided. The second step is to procure provisioning information from the resource description. In this case, the sensor type and its domain of operation are used to provision. That combination is then sent to a cloud platform where the M3 framework is deployed. It creates an application template which contains all components for the data processing, semantic reasoning, data management and

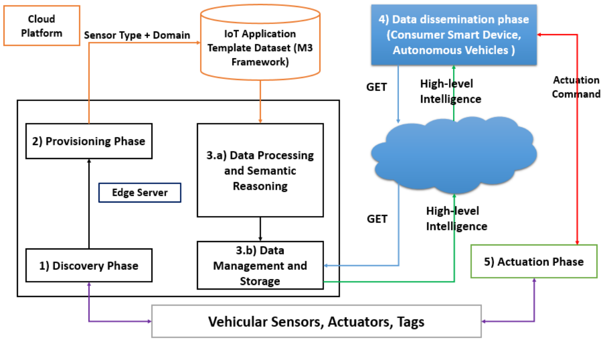

Cloud Platform
Sensor Type + Domain
IoT Application Template Dataset (M3 Framework)
4) Data dissemination phase (Consumer Smart Device, Autonomous Vehicles)
GET
High-level Intelligence
Actuation Command
2) Provisioning Phase
3.a) Data Processing and Semantic Reasoning
Edge Server
GET
High-level Intelligence
1) Discovery Phase
3.b) Data Management and Storage
5) Actuation Phase
Vehicular Sensors, Actuators, Tags

Fig. 3. IoT Framework to Connected Vehicles in an IoT ecosystem

repository. This step efficiently hides the complexity of IoV application development from developers and minimizes the time-to-market. The high level intelligence can be disseminated using RESTful interactions and actuation command can be initiated by the consumers.

D. Integration in the ETSI ITS architecture

The IoT architecture previously described does not depend on an underlying access technology. But to use it with vehicles and for the use cases described in Sect. II-A, the architecture may be integrated with the ETSI ITS architecture as shown in Fig. 4, where IoT-Fog, NDN and PVD blocks correspond to IoV extensions to ITS.

The Combined architecture is proposed to include the IoT elements along with ETSI ITS architecture elements. Vehicular resources for sensing, NDN for data dissemination, an IoT facilities layer along with Local Dynamic Map (LDM) and IoT/ITS application layers are introduced into the combined architecture.

Most of the IoT-related functions are located at the Facilities layer, and although being described for the European architecture, the IoT-related mechanisms and APIs are highly likely to be similar in the US counterpart. Although IEEE 1609.0-2016 describes the existence of such Facilities Layer, to the best of our knowledge, a standard does not exist in IEEE 1609. It is also expected that such Facilities and accordingly IoT extensions not to be integrated in IEEE 1609, but rather in an extension of the J2945.x set of SAE standards. This will be subject to a subsequent investigation.

The Access and Networking & Transport layers are transparent in our architecture, although the NDN stack is currently not supported by the ETSI ITS architecture. The ”Facilities” layer contains an *IoT Fog* block, which integrates most of the IoV elements described in Fig. 2. Four main APIs are required, one for the *Vehicular Resources*, one for the *IoV Applications*, one for the *IoV Data Dissemination*, and one for the LDM, which will need to be extended to support the *Data Management & Storage* functions. The ”Applications” contains the main IoV application logic.

The APIs connecting the two architectures elements form the stepping stone towards interoperability between the two architectures.

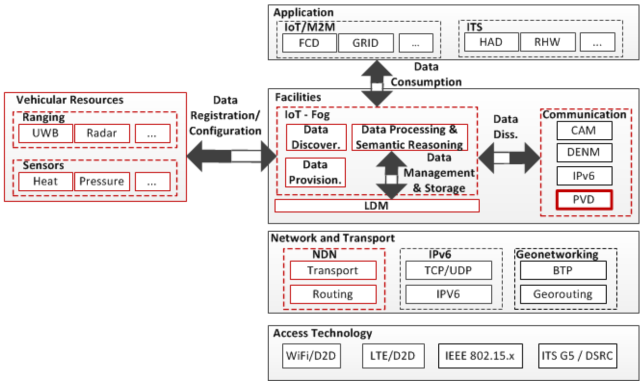


Fig. 4. IoT and ETSI ITS architecture integration

E. Solving Identified Challenges

The components of the presented IoT architecture provides solutions for the limitations and challenges identified in our IoV landscape and state-of-the-art analysis. The lack of data-oriented networking is solved by the ”data-centric” approach of the architecture itself. Also inclusion of NDN elements for data dissemination brings the focus on data-centric networking. The edge computing support necessary for IoV scenarios will be provided by the generic processing and storage layer depicted in Fig 2. With respect to the combined architecture, the IoT-Fog elements in the ”Facilities” layer are dedicated to this task. Seamless interoperability among vehicular resources, computing platforms and consumer devices are mainly handled by utilizing open standards (e.g. SenML, oneM2M, W3C) and semantic web technologies through the M3 framework which is itself following the best practice of ETSI M2M and oneM2M specifications. The developers should consider the five phases depicted in Fig. 3 which leads to best practice guidelines to create IoV applications.

V. Conclusions

In a nutshell, the paper motivates the emerging and highly multidisciplinary ecosystem of IoV. The next phase of evolution in automotive industry will be defined by consumer centric IoV applications and services. Vehicles and consumers participating to the IoV ecosystem will generate tons of raw data. The auto OEMs will need to collect and derive intelligence from the raw data and provide value to the consumers through the modern ”sharing-based” economy. Our IoT architecture considers additional enablers like Edge and Cloud platforms, smartphones and powerful OBUs. Seamless interoperation among the architecture components will be the key force driving the adaption of IoV. Our IoT architecture and its functional components provide a complete solution to enable the IoV based Auto 3.0 scenarios. Our main contribution is in addressing the challenges with most expected impact e.g. data driven nature, seamless interoperability and coexistence of cloud and fog platform. An additional impact is the framework and guidelines to ease IoV application development. With that, we anticipate IoV will evolve towards generating a collaborative awareness, strong social impact and cognition among consumer, vehicles and computing platforms in future.

VI. Acknowledgments

This work has been partially funded through the French ANR research project Data Tweet (ANR-13-INFR-0008) and the EU H2020 HIGHTS project (636537-H2020). EURECOM acknowledges the support of its industrial members, namely, BMW Group, IABG, Monaco Telecom, Orange, SAP, ST Microelectronics, and Symantec.

References

[1] S. Abdelhamid, H. S. Hassanein, and G. Takahara. Vehicle as a resource (vaar). *IEEE Network*, 29(1):12–17, Jan 2015.

[2] S. K. Datta and C. Bonnet. A lightweight framework for efficient m2m device management in onem2m architecture. In *Recent Advances in Internet of Things (RIoT), 2015 International Conference on*, pages 1–6, April 2015.

[3] S. K. Datta and C. Bonnet. Describing things in the internet of things: From core link format to semantic based descriptions. In *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pages 1–2, May 2016.

[4] S. K. Datta, C. Bonnet, and J. Haerri. Fog computing architecture to enable consumer centric internet of things services. In *2015 International Symposium on Consumer Electronics (ISCE)*, pages 1–2, June 2015.

[5] S. K. Datta, R. P. F. D. Costa, and C. Bonnet. Resource discovery in internet of things: Current trends and future standardization aspects. In *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pages 542–547, Dec 2015.

[6] M. Gerla. Vehicular cloud computing. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean*, pages 152–155, June 2012.

[7] A. Gyrard, S. K. Datta, C. Bonnet, and K. Boudaoud. Cross-domain internet of things application development: M3 framework and evaluation. In *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on*, pages 9–16, Aug 2015.

[8] P. Jaworski, T. Edwards, J. Moore, and K. Burnham. Cloud computing concept for intelligent transportation systems. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pages 391–936, Oct 2011.

[9] K. Mershad and H. Artail. Crown: Discovering and consuming services in vehicular clouds. In *Communications and Information Technology (ICCIT), 2013 Third International Conference on*, pages 98–102, June 2013.

[10] S.-H. Seo, T.-Y. Moon, J.-H. Kim, S.-H. Hwang, and J. W. Jeon. Smart vehicle management system by using gateway, hand-set and vmp. In *Control, Automation and Systems, 2007. ICCAS '07. International Conference on*, pages 1509–1513, Oct 2007.

[11] J. Soryal and T. Saadawi. Dos attack detection in internet-connected vehicles. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 7–13, Dec 2013.

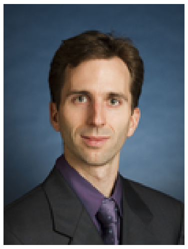
[12] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song. Toward a standardized common m2m service layer platform: Introduction to onem2m. *IEEE Wireless Communications*, 21(3):20–26, June 2014.

[13] A. Vinel, W. S. E. Chen, N. N. Xiong, S. Rho, N. Chilamkurti, and A. V. Vasilakos. Enabling wireless communication and networking technologies for the internet of things [guest editorial]. *IEEE Wireless Communications*, 23(5):8–9, October 2016.

[14] J. Wang, J. Cho, S. Lee, and T. Ma. Real time services for future cloud computing enabled vehicle networks. In *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, pages 1–5, Nov 2011.

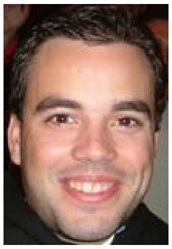
[15] J. Wang, Y. Liu, and W. Gao. Securing internet of vehicles using tcm. *JDCTA*, 4(7):226–233, 2010.

Soumya Kanti Datta is a Research Engineer and joined EURECOM in 2012. His research focuses on innovation, standardization, development of next-generation technologies in Internet of Things, Connected Cars and Smart Cities. He has contributed to three FUI Pole SCS projects (Smart 4G Tablet, WLBox 4G, Platform Telecom), an ANR project (DataTweet) and is currently working on H2020 HIGHTS project. He is an active member of IEEE and IEEE Consumer Electronics Society. He has published more than 50 research papers and articles in top IEEE Conferences, Magazines and Journals. Soumya has served in top IEEE conferences in many capacities. Currently he is involved in oneM2M and W3C Web of Things Standards Group and contributing to their standard development activities. He holds an MS degree from Telecom ParisTech (EURECOM), France.



Jérôme Härri is an Assistant Professor at the Communication System Department at EURECOM, France, and conducting research in wireless vehicular networks. Previously, he led the Traffic Telematics Junior Research Group at the Institute of Telematics of the Karlsruhe Institute of Technology (KIT), Germany. His research interests are related to the optimization of the vehicular wireless channel usage, to the investigation of cooperative ITS strategies and to the characterization of the mutual relationship between vehicular mobility and heterogeneous vehicular communication. He has authored and co-authored over 60 international journal and conference papers, and is involved in various National and European research projects related to wireless vehicular communications. He holds a M.Sc. degree (2002) and a Dr. ès sc. (PhD) degree (2007) in telecommunication from the Swiss Institute of Technology (EPFL), Lausanne, Switzerland.

Prof. Christian Bonnet joined EURECOM in 1992 after more than 12 years in industry. He was at the head of the Mobile Communications Department of EURECOM from 1998 to 2011. He is currently leading the Wireless Systems and Protocols research group. He participated in many (FP5, 6, 7, H2020) European projects dealing with mobility features based on IPv6 in heterogeneous mobile systems, Software defined Radio, Mesh architectures for public safety systems. His current field of research is on M2M and Internet of Things. He is leading the president of the open source OpenAirInterface Software Alliance targeting 5G systems. He is the technical coordinator of several French national projects mixing LTE access and M2M services. He is involved in the Secured Communicating Solutions regional cluster for innovation as co-leader of the Mobiles services and M2M strategic axe. He co-authored more than 200 publications in International conferences.



Rui Pedro Ferreira da Costa was born in Portugal in 1984. He received his MsC in Computers and Telematics from the University of Aveiro (Aveiro, Portugal) in 2008 and his PhD degree in Computer Science and Networks from Telecom ParisTech (Paris, France) in 2014, under the topic of "Mobility Architecture for Next Generation Networks". His main focus of research consisted of Mobile Networks, Vehicular Networks and Internet of Things. Rui developed this work as part of the post-doctoral program he attended at EURECOM. Currently he works in the field of satellite communications.