Internet of Vehicles Functional Architectures - Comparative Critical Study

Eugen Borcoci, Serban Obreja, Marius Vochin
University POLITEHNICA of Bucharest - UPB
Bucharest, Romania
Emails: eugen.borcoci@elcom.pub.ro, serban@radio.pub.ro, mvochin@elcom.pub.ro

***Abstract* — The continuous growth of the vehicles number, together with associated problems encountered in transportation systems have driven significant developments in the framework of Intelligent Transport System (ITS). Recently, an advanced solution - Internet of Vehicles (IoV) is proposed, seen as a part of Future Internet and specifically of Internet of Things (IoT), aiming to offer novel advanced commercial and technical capabilities. IoV will integrate the previous Vehicular Ad Hoc Networks (VANET) and also functionalities already developed in ITS. However, the architectural aspects of the IoV are still open research issues. This paper attempts a comparative critical study of several functional architectures proposed for IoV, including recent ones based on Cloud/Fog computing and Software defined networking (SDN) - control.**

Keywords — Internet of Vehicles, VANET; Cloud computing; Fog computing; Software Defined Networking; Network Function Virtualization.

I. INTRODUCTION

The vehicular communications have been intensively studied, designed, standardized and implemented in the last two decades. The umbrella and framework for such developments is the *Intelligent Transport System* (ITS) [1][2]. Associated technologies are *Dedicated Short-Range Communications* (DSRC) and *Wireless Access in Vehicular Environments* (WAVE) [2]. IEEE 802.11p and IEEE 1609 represent a set of standards for DSRC/WAVE networks.

Vehicular Ad Hoc Networks (VANET) [1] have been defined to support basic vehicular communications: vehicle to vehicle (V2V), vehicle to road (V2R), or vehicle to Infrastructure (V2I). The initial VANET components are the *On-Board-Unit* (OBU) placed in the vehicles and *Road-Side–Unit* (RSU) placed on the roads. The RSUs can inter-communicate and also could be linked to external networks like Internet. The main applications of VANET have been oriented to safety and traffic management applications.

The VANETs have several limitations related to their pure ad hoc network architecture (in V2V case), unreliable Internet service, incompatibility with personal devices, non-cooperation with cloud computing, low accuracy of the services, operational network dependency and restricted areas of applications and services. Therefore, extending the VANET architecture is considered today as a strong need.

Recently, *Internet of Vehicles* (IoV) has been proposed as a significant enhancement in vehicular communication area. It could be seen as a global span of a vehicle network [3][4]. The IoV is considered as a special case of *Internet of Things* [5][6], where the “things” are either vehicles or their subsystems. The IoV will connect the vehicles and RSUs through different *Wireless/Radio Access Technologies* (WAT/RAT), while traditional Internet and other heterogeneous networks will be used for wide area. The IoV objectives can include the traditional VANET services but also novel ones, e.g., vehicle traffic management in urban or country areas, automobile production, repair and vehicle insurance, road infrastructure construction and repair, logistics and transportation, etc. The IoV can be supported by recent technologies like centralized *Cloud Computing* (CC) combined with *Fog* or *Edge Computing* [7]; the latter can offer a better time response, more flexibility and degree of functional distribution, which are more appropriate for vehicular world.

In terms of management and control, *Software-defined networking* (SDN) [8] can offer to IoV its centralized up-to-date logical view upon the network, programmability, facilitating a flexible network management and on-the-fly modification of the network elements behavior. *Network Function Virtualization* (NFV) [9] can add flexibility by virtualizing many network functions and deploying them into software packages. Dedicated *Virtualized Network Functions* (VNF) can be defined, then dynamically created/destroyed, assembled and chained to implement legacy or novel services. NFV can cooperate with SDN to realize new flexible and powerful IoV architectures.

The large communities of users/terminal devices in IoV need powerful and scalable *Radio Access Technologies* (RAT). The 4G and the emergent 5G, based on cloud computing architectures (*Cloud Radio Access Network*-CRAN) are significant candidates for constructing the IoV access infrastructure [10].

Despite IoV promises high capabilities, there still exist many challenges, both in conceptual and architectural aspects and also from implementation and deployment point of view. Many IoV advanced features and integration with the above technologies (CC, Fog, SDN, NFV) are still open research issues.

This paper attempts a comparative critical study of several functional architectures proposed for IoV, including recent ones based on Cloud/Fog computing and Software *defined networking (SDN) - control. An enriched functional architecture with Fog computing and SDN control is proposed.*

The paper is organized as follows. Section II is an overview of related work with a critical presentation of some IoV generic architectures. Section III revisits the SDN-based architectures of IoV. Section IV proposes an enriched integrated architecture, Fog-SDN oriented. Section V presents conclusions and future work.

II. IOV GENERIC LAYERED ARCHITECTURES EXAMPLES

IoV is usually seen as a part of the more general Internet of Things (IoT), so it is of interest to evaluate how the proposed IoV architectures are generally consistent with IoT architecture.

Al-Fuqaha et al. [5] present an overview of IoT, identifying the Iot elements, i.e., *identification, sensing, communication, computation, services and semantics.* Several variants of IoT layered architectures are presented, where the most comprehensive has 5-layers: *Objects (perception) (OL), Object Abstraction (OAL), Service Management (SML), Application (AL)* and *Business (BL)* layer. These layers are different from those of the classical TCP/IP architectures, but the layering principles are still preserved.

The *Object* layer represents IoT physical sensors and actuators, performing functionalities such as querying location, temperature, weight, motion, vibration, acceleration, humidity, etc. The digitized data are transferred to the OAL through secure channels.

The *Object Abstraction* layer transfers data to the SML through secure channels. Layer 2 networking transfer functions are included here, based on technologies like RFID, GSM, 3G, 4G, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, etc. Additionally, cloud computing functions and data management processes are handled at this layer. The *Service Management* layer plays a middleware role, by pairing a service with its requester based on addresses and names. The SML supports IoT application programmers to work with abstracted heterogeneous objects. It also processes received data, takes decisions, and delivers the required services over the network wire protocols. The *Application* layer provides to the customers the requested services (with appropriate quality). The AL covers different vertical markets (e.g., smart home, smart building, transportation, industrial automation and health care, etc.). The *Business Layer* manages all IoT system activities and services. Using data provided by AL, it creates a business model, graphs, flowcharts, etc.; it is related to design, analysis, implementation, evaluation, monitoring and management (of the lower layers), and developing IoT system related elements. Decisions can be taken following Big Data analysis. Security features are included. Note that the architecture described above is a high level view only; further structuring can be made and mapping on various existing protocols [5].

For IoV, several architectures are recently proposed and discussed. A short critical overview and comparison is exposed below.

Bonomi et al. [6] proposed a four - layered architecture for connected vehicles and transportation. The layers are also called *"IoT key verticals",* suggesting that a given layer includes not only classical layer functions (i.e., L1, L2,…) but rather groups of functions, which could be mapped on several classical layers. Also, the four layers are rather corresponding to different geo-locations of the subsystems (vehicles, networking infrastructure, cloud data centers, etc.) The bottom layer (*end points*) represents the vehicles, plus their communication protocols (basically for V2V communication, using the IEEE 802.11p). The layer two (*infrastructure*), represents communication technologies to interconnect the IoV actors (via WiFi, 802.11p, 3G/4G, etc.). The third layer (*operation*) performs management actions; it verifies and ensures compliance with all applicable policies, to regulate the information management and flow. The fourth layer is called *cloud* (public, private or enterprise) based on a defined profile coupled with the possibility of receiving services (voice, enterprise video and data) on demand. Note that this architectural view is a mixed one, and does not clearly separate the sets of functions of different levels.

Kayvartya et al. [4] have proposed an IoV five layer architecture, to support an enriched set of vehicular communications, in addition to traditional V2V, V2R/V2I, i.e., *Vehicle-to-Personal* devices (V2P) and *Vehicle-to-Sensors* (V2S). Each particular IoV communication type can be enabled using a different WAT, e.g., IEEE WAVE for V2V and V2R, Wi-Fi and 4G/LTE for V2I, CarPlay/NCF (*Near Field Communications*) for V2P and WiFi for V2S. The system includes vehicles and *Road Side Units* (RSU), but also other communication devices. Embedding such a large range of devices makes IoV more complex, (compared to VANET), but more powerful and market oriented.

Three architectural planes are defined: *management*, *operation* and *security*. The network model is composed of three functional entities: *client, connection* and *cloud.* The layers are (see Figure 1): *perception, coordination, artificial intelligence, application* and *business.*

The *perception* layer (PL) functions generally correspond to those of the traditional physical layer. The PL is instantiated by *sensors* and *actuators* attached to vehicles, RSUs, smart-phones and other personal devices. Its main task is to gather information on vehicle, traffic environment and devices (including movement –related parameters).

The *coordination* layer (CL) represents a virtual universal network coordination entity for heterogeneous network technologies (WAVE, Wi-Fi, 4G/LTE, satellites). While the basic job is transportation, some other processing tasks are added, of information received from heterogeneous networks with aim to create a unified structure with identification capabilities for each type of network.

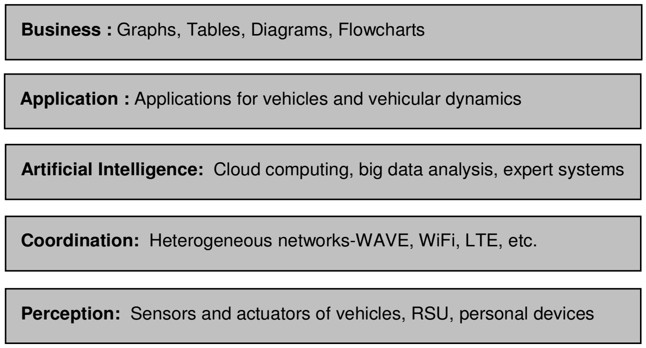

Figure 1. Five layer IoV architecture [4].

The *artificial intelligence* layer (AIL) is represented by a generic virtual cloud infrastructure, working as an information management centre. It stores, processes and analyzes the information received from the lower layer and then takes decisions. Its major components are: *Vehicular Cloud Computing (VCC), Big Data Analysis (BDA)* and *Expert System.* The AIL should meet the requirement of applications and services working on top of it.

The *application* layer (AL) contains smart applications (e.g., for traffic safety and efficiency, multimedia-based infotainment and web based utility). The AL include safety and efficiency applications (VANET legacy) and provides smart services to End Users (EU) based on intelligent analysis done by AIL. The AL efficiently discovers the services provided by AIL and manage their combinations. It also provides EU application usage data to the business layer. Currently, it is recognized that these smart applications constitute a major driving force to further develop IoV.

The *business* layer (BL) includes IoV operational management functions, basically related to business aspects: to foresight strategies for the development of business models based on the application usage data and statistical analysis of the data; analysis tools including graphs, flowcharts, comparison tables, use case diagrams, etc.; decision making - related to economic investment and usage of resources; pricing, overall budget preparation for operation and management; aggregate data management.

The architecture is split in three parallel planes: *operation, management and security.* The work [4] also proposed a possible mapping between the five layers and different protocols already developed in vehicular communications by ITS, VANET, IEEE, etc. The *operation* plane contains actually traditional *data* plane functions but still has some control and management role.

At *perception* layer, current technologies can be used for access in ITS and VANET (see Figure 2). However, the CL includes not only TCP/IP transport and network protocols but also different solutions (with no IP usage). Examples are: IEEE 1609.4 along with a *Global Handoff Manager* (GHM-open research) and other protocols proposed at network layer in projects like CALM, WAVE. For instance, in the stack there exist WSMP - Short Message Protocol and FAST -Fast Application and Communication Enabler.

In AIL, cloud capabilities are seen as major contributors, working on top of lower sub-layer: CALM Service Layer (CALM-SL) and WAVE-1609.6 service related protocols. The upper sub-layer consists in Vehicular Cloud Computing (VCC) and Big Data Analysis (BDA) related protocols. They can offer cloud services of type "*X as a Service*": Storage (STaaS), Infrastructure (INaaS), Network (NaaS); Cooperation (CaaS), Entertainment (ENaaS), Gateway (GaaS); Picture (PICaaS) and Computing (COMaaS).

Still further research work is necessary, given the current unavailability of enough suitable protocols for VCC and BDA. Another open issue is that VANETs projects, generally, do not have clear definitions of the upper sub-layer, while some IoT projects are recently working towards these.

The *Application Layer* (AL) includes two sets of applications: *Smart Safety and Efficiency* (SSE) and *Smart Business Oriented* (SBO). The current WAVE resource handler protocol 1609.1 can be used on the top of these applications, to manage the resources among smart applications. The *Business Layer* (BL) in [4] proposes various business models like Insurance (INS), Sale (SAL), Service (SER) and Advertisement (ADV). The set of these functionalities could be further enriched in the future.

The architecture has the merit that integrates in the management and security planes some existing functional blocks and protocols (see Figure 2), already developed in WAVE (P1609.x), CALM and C2C projects.

However the mentioned 5-layer architecture does not touch some important and recent aspects in developing IoV architecture, e.g., how to distribute computation intelligence between a central cloud and fog units (which are placed at the network edge) while cloud-fog combination seem to be an efficient and attractive solution for a distributed system like IoV. Also, SDN-like control possibilities are not discussed in this architecture.

Contreras-Castillo et al. [11] propose a seven layer architecture, supporting the functionalities, interactions, representations and information exchanges among all the devices inside a IoV ecosystem. The authors claim that this architecture (having more than five layers) has as objective to reduce the complexity of each layer and better standardize the interfaces and protocols used in each layer. The interaction model considers the following entities which can communicate to each other: vehicle (V), person (P), personal device (P), network infrastructure (I), sensors (S), any device (D) and roadside device (R). Consequently, the communications might be of type V2V, V2R, V2I, V2D, V2P, V2S, D2D.

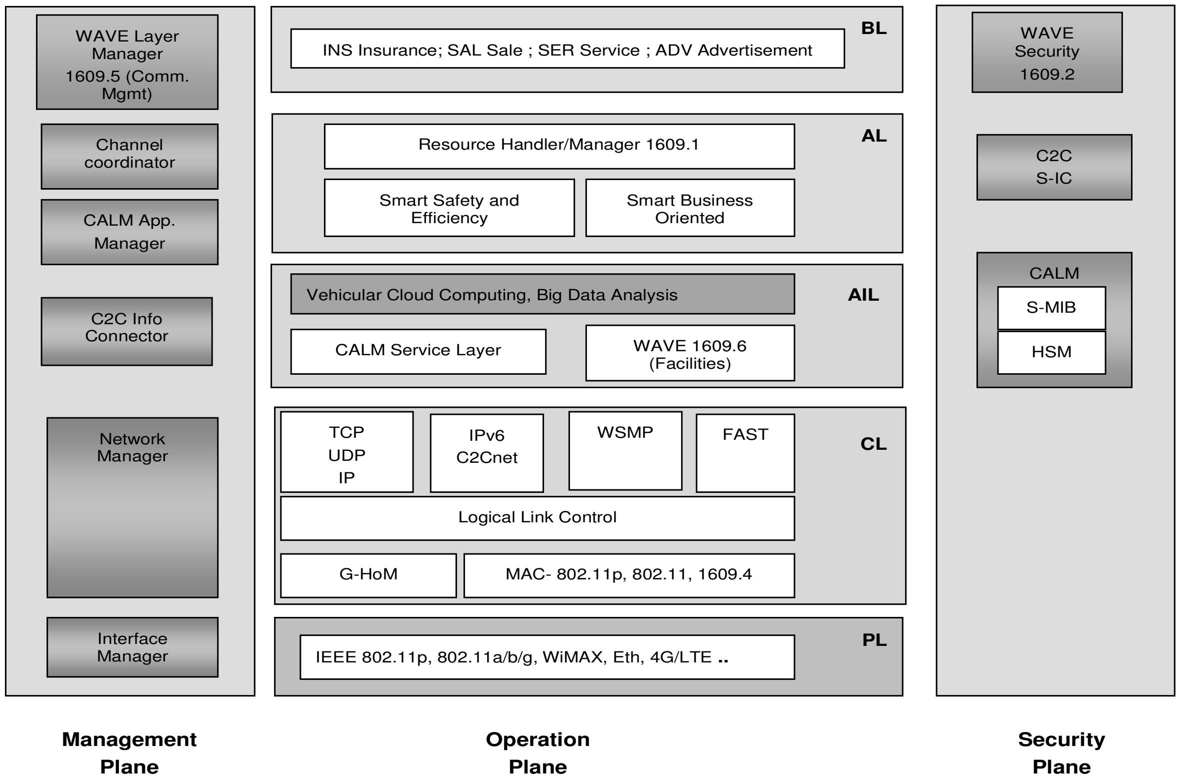

Figure 2. Five layer IoV architecture mapped on particular protocols [4]

PL Perception layer; CL Coordination layer; AIL Artificial Intelligence layer; AL Application layer; BL Business layer; C2C Car to Car; CALM Communication Architecture for Land Mobile; DSRC Dedicated Short Range Communication; WAVE Wireless Access in Vehicular Environment; FAST Fast Application and Communication Enabler; LLC Logical Link Control; G-HoM Global Handoff Manager; WSMP WAVE Short Messages Protocol; BDA Big Data Analysis; VCC Vehicular Cloud Computing; SSE Smart Safety and Efficiency; SBO Smart Business Oriented; INS Insurance; SAL Sale ; SER Service ; ADV Advertisement; HSM Hardware Security Manager; S-IC Security Information Connector; S-MIB Security Management Information Base

The network model should support collaboration between multi-users, multi-vehicles, multi-devices (sensors, actuators, mobile devices, access points), multi-communication models (point to point, multi-point, broadcast, geo-cast) and multi-networks (wireless or wire networks with various technologies like WiFi, Bluetooth, WiMAX, 3G, 4G/LTE, etc.).

The layers defined in [11] are (bottom-up list): *User interaction, Data acquisition, Data filtering and pre-processing, Communication, Control and management, Business and Security.*

Note that this "layered" architecture actually does not follow the principles of a layered stack architecture (where each layer traditionally offers some services to the above one). For instance, the *Control and management layer* and *Security* layer seem to be rather architectural "planes "and not traditional layers; they have to interact with all other five layers. No notion of an architectural "plane" is explicitly defined in [11].

The *User interaction* layer contains in-vehicle computing systems including: a. information-based systems to provide information (e.g., on routes, traffic conditions, car parking availability and warning/advice regarding risks) to components of the driving environment, the vehicle or the driver; b. control-based systems to monitor changes in driving habits and experiences and operational elements of the driving task (e.g., adaptive cruise control, speed control, lane keeping and collision avoidance). It is stated in [11] that designing user interfaces for in-vehicle systems is still posing many new research challenges. Note that this "layer" actually contains functions of several layers defined in other architectures (e.g., some structured in a similar way as classic TCP/IP stack).

The *Data acquisition* layer has tasks covering all three traditional planes (data, control and management). Apparently it overlaps functions of "networking" Layer 2. It gathers data (for safety, traffic information, infotainment), from a given area of interest, from all the sources (vehicle's internal sensors, GPS, inter-vehicle communication, Wireless Sensor Networks (WSN), or devices such as cellular phones, sensors and actuators, traffic lights and road signals located on streets and highways. Intra- and inter vehicular interactions are within the scope of this layer. Various access technologies and associated protocols are supposed to perform the tasks. For intra-vehicle communication, the proposals are: Bluetooth (2.4 GHz) , ZigBee(868 MHz, 915 MHz and 2.4 GHz) Wi-Fi HaLow (900 MHz) Ultra-wideband (3.1–10.6 GHz), with data rates up to 480 Mbps and coverage distances up 1000m. For inter-vehicles communication technologies can be: IEEE WAVE/DSRC with IEEE 802.11p for PHY and MAC layers and the IEEE 1609 family for upper layers; 4G/LTE (1700 and 2100 MHz).

The *Data filtering* and *pre-processing* layer is necessary, given that IoV, may generate huge amounts of data, not all being relevant for all entities. This layer analyses and filters the collected information, to avoid the dissemination of irrelevant information and reduce the network traffic. Examples of protocols to be used in this layer are: *Xtensible Messaging and Presentation Protocol* (XMPP), *Constrain Application Protocol* (CoAP), *HTTP Representational State Transfer* (HTTP REST), *Message Queuing Telematic Transport* (MQTT), *Lightweight Local Automation Protocol* (LLAP). Several data filtering approaches are referenced in [11], but novel intelligent and efficient data mining techniques are considered to be necessary.

The *Communication* layer actually performs both data and control function at networking level, given the set of protocols suggested as: 6LoWPAN, IPv4, IPv6, Routing Protocol for Low Power and Lossy Networks (RPL), etc. This layer should select the best network to send the information, based on several selection parameters.

The *Control and management* layer is the global coordinator for managing different network service providers within the IoV environment. Its functions are: to manage the data exchange among the various services; to manage the information generated by devices: in-vehicle or around sensors, roadside infrastructure and user devices in the environment; apply different suitable policies (e.g., traffic management and engineering, packet inspection, etc.)

The *Business* layer processes information using various types of cloud computing infrastructures locally and remotely. Typical functions are: storing, processing and analysing info received from the other layers; making decisions based on data statistical analysis and identifying strategies that help in applying business models based on the usage of data in applications and the statistical analysis. (tools such as graphs, flowchart, critical analysis, etc.). The protocols proposed for this layer are: *CALM Service Layer*, WAVW 1609.6, TR-069, *Open Mobile Alliance Device Management* (OMA-DM).

The *Security* layer (despite of its naming of “layer”) is actually an architectural plane which communicates directly with the rest of the layers. It implements security functions (data authentication, integrity, non-repudiation and confidentiality, access control, availability, etc.) to exchange data among sensors, actuators, user’s devices through secure networks and service providers. The protocols envisaged are similar to those presented in Figure 2.

The seven layer architecture of [11] does not touch the integration of SDN/NFV approach. The cloud services are located at business level (as vehicular cloud computing) while we believe that a more natural placement could be as in Figure 2, i.e., under application layer. Some mixture of “layers” and “plane” notions is apparent; there is a lack of enough orthogonality of different “layers”.

III. SDN CONTROLLED IOV ARCHITECTURES

This section shortly presents related work dedicated to VANET/IoV with SDN control.

Y.Lu et al. [12] applies SDN control to VANET, to get more flexibility, programmability and support for new services. The architectural components are: SDN controller, SDN wireless nodes and SDN- enabled RSUs. The SDN controller is a single entity performing the overall control of the system. The SDN wireless nodes are vehicles, seen as data plane elements (SDN - forwarders). The SDN RSUs are also treated as data plane elements, but hey are stationary. The benefits of the approach are proved by simulation, while considering some specific use cases (e.g., routing). However, a complete layered functional IoV architecture is not discussed.

K.Zeng et al. [13] propose an IoV architecture called *software-defined heterogeneous vehicular network* (SERVICE), based on Cloud-RAN technology, able to support the dynamic nature of heterogeneous VANET functions and various applications. A multi-layer Cloud-RAN multi-domain is introduced, where resources can be exploited as needed for vehicle users. The system is hierarchically organized (there are defined: remote, local and micro clouds) and virtualization (for flexibility) is considered for implementation. The high-level design of the soft-defined HetVNET is presented. The SDN control is organized on two levels (one primary controller and several secondary controllers; each one of the latter controls a given service area). A complete layered functional IoV architecture is not in the paper scope.

A Fog-SDN architecture called FSDN is proposed for advanced VANET by Truong et al. [7], for V2V, V2I and Vehicle-to-Base Station communications. The Fog computing brings more capabilities for delay-sensitive and location-aware services. The SDN components are: *SDN Controller* (it controls the overall network behavior via *OpenFlow* –interfaces; it also plays as Orchestration and Resource Management for the Fog); *SDN Wireless Nodes* (vehicles acting as end-users and forwarding elements, equipped with OBU); *SDN RSU* (it is also a Fog device); *SDN RSU Controller* (RSUC) (controlled by the central SDN controller; each RSUC controls a cluster of RSUs connected to it through broadband connections. The RSUC can forward data, and store local road system information or perform emergency services. From Fog perspective RSUCs are fog devices); *Cellular Base Station* (BS) performing traditional functions (they are SDN-controlled via OpenFlow and can also offer Fog services). This study does not discuss a full functional layered IoV architecture.

Kai et al. [14] present an overview of Fog–SDN solution for VANET and discuss several scenarios and issues. It is shown that a mixed architecture Fog-SDN (similar to that

 ISBN: 978-1-61208-583-8

proposed in [7]) can be powerful and flexible enough, to serve future needs of IoV. Again, we note that this study does not discuss a full functional layered IoV architecture.

Chen et al. [15] discusses an IoV architecture and solutions based on SDN control. However, a full functional layered architecture is not discussed.

IV. SDN-FOG ENABLED IOV FUNCTIONAL ARCHITECTURE

This section proposes a layered functional IoV architecture of a heterogeneous network including SDN control and Fog capabilities. We propose a possible infrastructure (Figure 3), which could be a horizontal extension of that proposed in [7]. The Data plane includes: mobile units (vehicles) equipped with OBUs; advanced RSUs, which could have enough resources (computing, storage) as to play also Fog role (F-RSU), or could be regular RSU like in traditional VANETs; base stations (BS) of type WiMAX/3G/4G-LTE. A fixed network (partial mesh) can interconnect the RSUs. The SDN Data plane contains the forwarding nodes and can be geographically organized in several service areas. The SDN Control plane is organized on two levels: primary SDN controller (P-SDNC) controlling the overall behavior of the network and secondary controllers (S-SDNC), one for each service area. The S-SDNC can also contain the resource management functions of the Fog infrastructure. The P-SDNC is logically connected to each S-SDNC via the Control plane overlay or physical links. The SDN south interfaces between the controllers and the lower level can be supported by OpenFlow protocol or similar. This infrastructure is enough general as to be considered as a candidate or IoV.

Figure 4 shows a proposal to enrich the layered functional architecture introduced in [4], by adding SDN and Fog functionalities, supposing that the infrastructure is that of Figure 3. The second layer is renamed in Network and Transport Layer (NTL), showing in a more explicit way the role of this layer. The Operation Plane is renamed in Control and Data Plane.

The functionalities of the P-SDNC can be embedded in the management plane, given that its role is to govern the overall network behavior (e.g some overall policies can be coordinated by this module). The regional SDN control is placed naturally at NTL level as to control the SDN forwarders and also the functions of Fog nodes located in the access area. Additionally S-SDNC functions can be included in the AIL, to serve this layer needs in terms of Fog AI resource control. The cloud services should be split between centralized Cloud computing and Fog nodes but this is out of scope of this study (it is for further work).

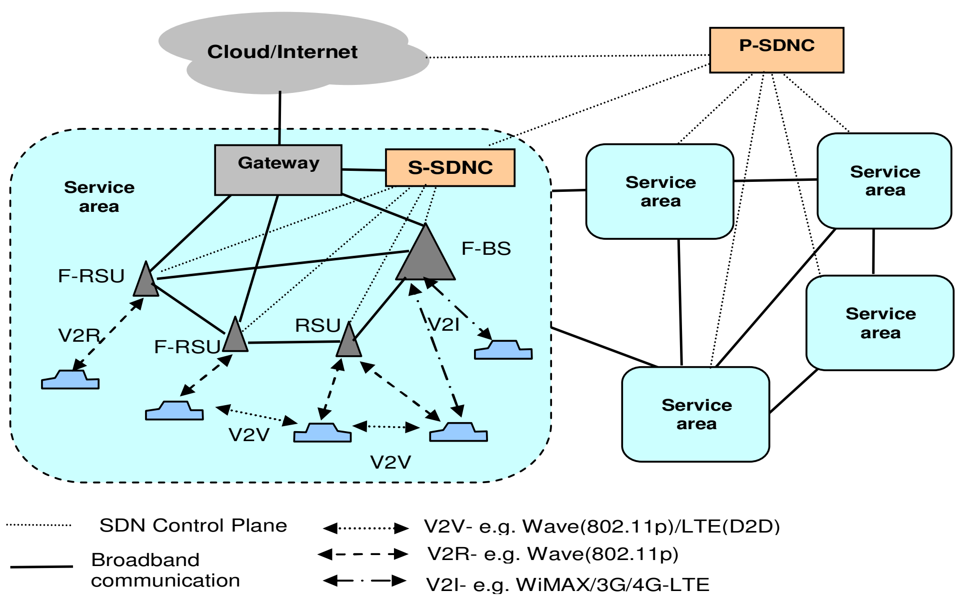

Figure 3. Generic IoV system architecture
F-BS - Fog-capable Base Station; F-RSU Fog-capable Remote Side Unit; P-SDNC- Primary SDN Controller; S-SDNC Secondary-SDN Controller; D2D- device to device communication

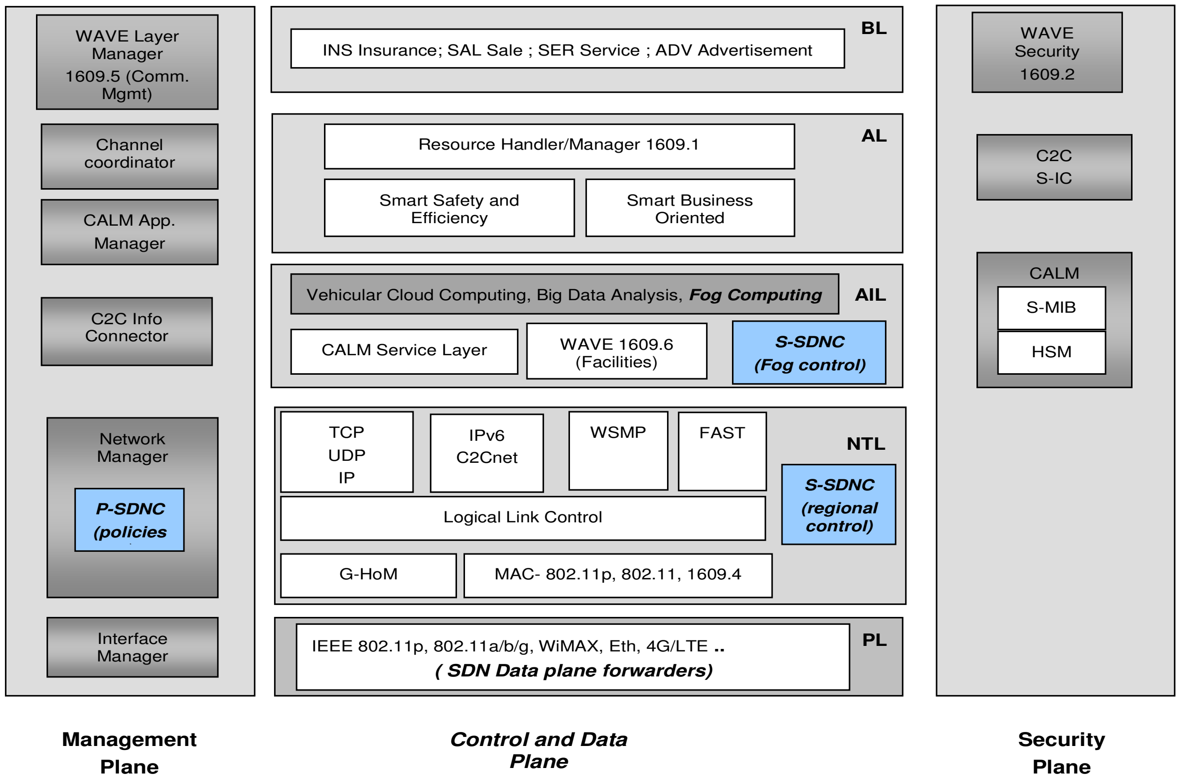

Figure 4. Functional IoV 5-layer architecture enriched with SDN control and Fog computing

V. CONCLUSIONS AND FUTURE WORK

This paper presented a comparative critical view of several IoV architectures proposed in the literature, focused on functional layering aspects. Among several proposals, we selected a five layer multiple-plane architecture, considering this model as a good and orthogonal approach which consistently include the major IoV functionalities and is giving the possibility to clearly define interfaces between layers and planes. The architecture is consistent with IoT architectural vision. In Section IV, a modified Fog-SDN based IoV infrastructure is proposed, where the associated layered architecture is enriched by considering the additional Fog-based approach and SDN distributed control. This work could be a contribution toward an IoV reference architecture.

Future work should be done to allocate and map different functions of the general functional layered architecture to specific entities of a complete IoV system. This should be done based on their different roles and placement: terminals (vehicles), RSUs, Fog Nodes, BS, core network, cloud data centers, etc. The virtualization aspects and their impact on the architecture are not discussed in this study. This is also a subject for further work.

VI. ACKNOWLEDGMENTS

This work has been partially funded by University Politehnica of Bucharest, through the “Excellence Research Grants” Program, UPB – GEX. Identifier: UPB–EXCELENȚĂ–2016 Research project Intelligent Navigation Assistance System, Contract number 101/26.09.2016 (acronym: SIAN).

REFERENCES

[1] S. Sultan, M. Moath Al-Doori, A.H. Al-Bayatti, and H.Zedan “A comprehensive survey on vehicular Ad Hoc Network”, J.of Network and Computer Applications, Jan. 2014, https://www.researchgate.net/publication/259520963, [Retrieved: December, 2016].

[2] Y. Li, “An Overview of the DSRC/WAVE Technology”, https://www.researchgate.net/publication/288643779, 2012, [Retrieved: May, 2017].

[3] Y. Fangchun, W.Shangguang, L. Jinglin, L. Zhihan, and S.Qibo, “An overview of Internet of Vehicles”, China Commun., vol. 11, no. 10, pp. 115, October 2014.

[4] O. Kaiwartya, A.H. Abdullah, Y. Cao, A. Altameem, and M. Prasad, “Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects” IEEE Access, Special Section on Future Networks, Architectures, Protocols and Applications, Vol. 4, pp.5536-5372, September 2016.

[5] A. Al-Fuqaha, M.Guizani, M. Mohammadi, M. Aledhari, and M.Ayyash, "Internet of Things: A Survey on Enabling

 ISBN: 978-1-61208-583-8

Technologies, Protocols, and Applications", IEEE Communications Surveys &Tutorials Vol. 17, No. 4, pp.2347-2376, 2015.

[6] F.Bonomi, R.Milito, J.Zhu, and Sateesh Addepalli, "Fog Computing and Its Role in the Internet of Things", August 2012, http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf, [Retrieved: January, 2017].

[7] N.N.Truong, G.M.Lee, and Y.Ghamri-Doudane, "Software defined networking-based vehicular ad hoc network with fog Computing", Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM'15), May 2015, Ottawa, Canada. Piscataway, NJ, USA: IEEE, , pp. 1202−1207, 2015.

[8] B. N. Astuto, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks", Communications Surveys and Tutorials, IEEE Communications Society, (IEEE), 16 (3), pp. 1617 – 1634, 2014.

[9] B.Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualisation: Challenges and Opportunities for Innovations". IEEE Communications Magazine, pp. 90-97, February 2015.

[10] M. Peng, Y. Li, J. Jiang, J. Li, and C.Wang, "Heterogeneous cloud radio access networks: a new perspective for enhancing spectral and energy efficiencies", IEEE Wireless Communications, pp.126-135, December 2014.

[11] J.C. Contreras-Castillo, et al., "A seven-layered model architecture for Internet of Vehicles",Journal of Information and Telecommunications , Vol. 1, No. 1, pp. 4–22, 2017.

[12] Y.Lu, M.Gerla, R. Gomes, and E. Cerqueira, "Towards software-defined VANET: Architecture and services", MedHocNet.2014.6849111, https://www.researchgate.net/publication/271472780, [Retrieved:April, 2017].

[13] K. Zeng, L. Hou, H. Meng, Q. Zheng, and N. Lu, "Soft-Defined Heterogeneous Vehicular Network: Architecture and Challenges", IEEE Network, vol. 30, pp.72-79, July/August 2016.

[14] K.Kai, W.Cong, and L.Tao, "Fog computing for vehicular Ad-hoc networks:paradigms, scenarios, and issues", The Journal of China Universities of Posts and Telecommunications, www.sciencedirect.com/science/journal/10058885, http://jcupt.bupt.edu.cn, 23(2), pp.56–65, April 2016, [Retrieved: January, 2017].

[15] J.Chen, H. Zhou, N. Zhang, P. Yang, L.Gui, and X. Shen, "Software defined Internet of vehicles: architecture, challenges and solutions", Journal of Communications and Information Networks Vol. 1, Issue (1): pp.14-26, 2016, DOI: 10.11959/j.issn.2096-1081.2016.002.