Towards the implementation of the Social Internet of Vehicles

(Article begins on next page)

26 April 2024

Towards the Implementation of the Social Internet of Vehicles

Luigi Atzori[a], Alessandro Floris[a], Roberto Girau[a], Michele Nitti[a], Giovanni Pau[b]

[a]DIEE, University of Cagliari, UdR CNIT of Cagliari, Italy
[b]LIP6, Sorbonne University, Paris, France

Abstract

The Internet of Vehicles (IoV) represents the emerging paradigm where vehicles are (almost) always connected to the Internet to deliver and receive information to/from other services so as to augment the knowledge and services the users can benefit from when moving in urban and rural areas by their vehicles, but not only. Furthermore, the exploitation of social networking notions into the IoV has brought to the definition of the Social IoV (SIoV) paradigm, i.e., a social network where every vehicle is capable of establishing social relationships in an autonomous way with other vehicles or road infrastructure equipments. In this paper, we propose an implementation of the SIoV leveraging on an existing cloud-based IoT platform to manage the social activity of the vehicles as defined by the SIoV paradigm. The contribution of the paper is multifold: i) we define some static and dynamic relationships that can be established between vehicles and road infrastructures taking part to the SIoV; ii) we show how the proposed system can be integrated into the standard Intelligent Transportation System Station Architecture (ITS SA); iii) we illustrate an effective low-cost and flexible solution for the On-Board Unit (OBU) to enable every vehicles to participate in the SIoV and create their own relationships; iv) we show the results of the conducted experimental tests for the creation of social relationships aimed at comparing the performance of Bluetooth and Wi-Fi technologies when used to manage vehicles' radio visibility. Finally, we present two use cases: the Vehicle Diagnostic and the Smart Parking applications.

Keywords: Vehicular Ad-hoc NETwork, Internet of Things, Social Internet of Vehicles, On Board Unit

1. Introduction

The main vision of the Internet of Things (IoT) is to enable every physical object in the real world, such as a room, a tree and a car, to communicate with any other object, in order to share information about their surrounding environment [1]. This is possible also thanks to the capability of smart objects to sense the environment through embedded sensors (as it is the case with smartphones and smart TVs) and to the availability of simple technologies for the identification of objects, such as Radio Frequency IDentification (RFID) and Near Field Communication (NFC). According to Cisco [2],

thanks to the fast spreading of these technologies, by 2020 every person will possess 6.58 connected devices on average.

Even before the advent of the IoT concept, vehicles were at the center of Intelligent Transportation Systems (ITS), whose objective is to make a smarter utilization of transport networks through the implementation of innovative services related to different modes of transportation, traffic management, road safety, etc. An increasing number of vehicles are now already equipped with advanced technologies that enable them to communicate with nearby vehicles creating Vehicular Ad-hoc NETworks (VANETs) [3]. Indeed, such vehicles are equipped with an On-Board Unit (OBU), which is used to communicate with other vehicles (Vehicle-to-Vehicle or V2V communications) or with Road-Side Units (RSUs) by employing wireless short-range technologies. The increasing interest around smart vehicles has a twofold motivation: on the one hand, several automotive manufacturers, such as Ford[1], Volvo[2], General Motors[3], are looking forward to designing a *future driverless car*; on the other hand, a smart car plays a crucial role for road safety and emergency situations and is able to offer a set of entertainment services to the final users through the use of cloud computing technology. These efforts led to a new branch in the IoT research community, which is focused on the creation of a global network of interconnected vehicles, namely the Internet of Vehicles (IoV) [4].

The IoV solutions inherit some of the issues related to the IoT. For example, searching for needed information, services and resources for the deployment of running applications exploiting the IoV infrastructure represents a crucial challenge: in addition to the size of the searching space, most of the sensors embedded in the vehicles produce data in real-time, making the system highly dynamic, as it happens for instance when tracking the position of the cars or monitoring the engine revolutions per minute or the intake manifold pressure. A further complication derives from the shift we are witnessing in the interaction model. From a paradigm where humans look for information provided by objects (human-object interaction), the IoV will surely move towards a model where vehicles look for other vehicles to provide composite services for the benefit of human beings (object-object interaction), such as the case where a platoon of vehicles collaborate to address traffic jams. With such an interaction model, it will be essential to understand how the information provided by the other vehicles have to be processed so as to build a trustworthy system on the basis of the behavior of the objects, otherwise attacks and malfunctions will outweigh any of the benefits of these technologies [5].

An approach with the potential to properly address the mentioned issues, which is recently gaining high popularity, is based on the exploitation of social networking notions into the IoV, as formalized by the Social IoV (SIoV) concept [6]. This is intended as a social network where every vehicle is capable of establishing social relationships with other vehicles or RSUs in an autonomous way with respect to the owner but ac-

---

[1]http://corporate.ford.com/innovation/research-and-innovation-center.html
[2]http://www.volvocars.com/intl/about/our-stories/human-innovations/our-future-thinking
[3]https://www.gm.com/mol/m-2016-may-0509-chevy-future.html

cording to the rules set by her. Every object can then interact with its friends when looking for some assistance, such as the provisioning of a piece of important information or a key service. This allows for the implementation of distributed and scalable procedures to manage object interactions in the same way as humans do when interacting in the social networks. The resulting process has a distributed nature, as each vehicle searches for its target peer among its friends, which, if unable to directly provide the requested service/information, takes further actions by inquiring their friends.

Although some articles have already taken into account the use of social relationships in IoV applications, to the best of our knowledge, no one has ever realized a complete SIoV implementation starting from the logic behind the socialization. In this paper, we set out to analyze all the problems that can be highlighted in the processes of creating relationships between dynamic objects, such as vehicles, and to propose solutions to facilitate the detection of new relationships. We propose an implementation of the SIoV on the basis of an existing cloud-based IoT platform and we build an OBU to make vehicles SIoV compliant. Finally, we show the results of experimental tests to verify the establishment of social relationships among vehicles. The presented experiments provide the basis to drive other studies on conducting further real experiments on the topic of SIoV, so as to avoid the shortcomings typical of studies based only on simulations.

The major contributions of this paper are the followings:

- We leverage on a cloud-based IoT platform, namely Lysis [7], to manage the social activity of the vehicles as defined by the SIoV paradigm. Accordingly, we describe the client middleware that has been developed to enable the vehicles to communicate with their virtual counterparts.

- We define some relationships that can be established between the vehicles taking part to the SIoV. These relationships can be either static, as the Parental Object Relationship established between vehicles belonging to the same automaker, or dynamic, as the Social Object Relationship established between vehicles that come into contact through V2V communications.

- We show how the proposed system can be integrated into the Intelligent Transportation System Station Architecture (ITS SA) defined by the ISO [8] and ETSI standards [9].

- We illustrate an effective low-cost and flexible solution for the OBU to enable every vehicles, even the ones without any kind of native connectivity, to participate in the SIoV and create their own relationships.

- We show the results of the conducted experimental tests for the creation of social relationships comparing the performance of Bluetooth, 802.11p and Wi-Fi technologies as wireless communication technologies to be used to manage vehicles' radio visibility. To this, we implemented the Local Neighbor Discovery (LND) algorithm presented in [39], which exploits the Wi-Fi/Bluetooth/802.11p radio interface scanning to detect beacons transmitted by static stations. When two vehicles are able to see the same beacon, then they are assumed to be close: after several encounters, two vehicles become friends.

3

- We present two use cases: a Vehicle Diagnostic and a Smart Parking application.

The rest of the paper is organized as follows. Section 2 presents the state-of-the-art works, while Section 3 describes the proposed implementation of the Social Internet of Vehicles. Section 4 presents the selected hardware and the implemented software to build an OBU compliant to the SIoV. In Section 5, we show the results of experimental tests for the creation of social relationships whereas in Section 6 we present two use cases: a Vehicle Diagnostic and a Smart Parking application. Finally, in Section 7 we draw some final remarks and lesson learnt.

2. Background

The Internet of Vehicles (IoV) can be seen as a natural evolution of Vehicular Ad hoc NETworks (VANETs) and the Social Internet of Vehicles (SIoV) is a vehicular instance of the Social IoT (SIoT), where the things are represented by cars, bicycles, trucks and buses in addition to Road Side Units (RSUs).

VANETs are usually classified as an application of Mobile Ad Hoc NETworks (MANETs) whose nodes are vehicles and RSUs. VANETs are characterized by high (variable) vehicle speed, hostile propagation environment, and quickly changing network topologies [3]. To create a VANET, vehicles are equipped with an On-Board Unit (OBU) through which they can communicate with other vehicles by building dynamically links (Vehicle-to-Vehicle or V2V communications) and with fixed RSUs (Vehicle-to-Infrastructure or V2I communications) [10]. V2V and V2I communications can employ different wireless short-range protocols, some of them specifically designed to work in this environment, such as the 802.11p, while other protocols, e.g. ZigBee, Bluetooth and Wi-Fi, are only used in specific situations since they need a longer connection time between vehicles w.r.t. 802.11p: these situations can be both statics, where for example a vehicle comes to halt at an intersection and wants to communicate with the traffic light, or mobile, when two vehicles move with similar speed. In this paper, we take into account another specific situation and tested Bluetooth and Wi-Fi for the sole purpose of creating a relationship between vehicles.

VANETs are very dynamic networks where some vehicles fall out of the signal range and drop out of the network while other vehicles can join in; therefore, vehicles are only involved temporarily, randomly and unsteadily in the VANETs so that their application range is usually local and discrete. As the number of connected vehicles to the Internet increases and thanks to the spreading of mobile cellular systems, vehicles become connected through an all IP-based infrastructure, which has led to the definition of the IoV concept [4, 11]. This concept envisages the intelligent integration of humans, vehicles, RSUs and environments which are capable of exchanging information directly or indirectly. As we enter in the IoT world, the possibility to create digital counterparts of any real object, namely the virtual objects, give the possibility to the vehicles to communicate not only through physical-physical paths but also through physical-virtual-virtual-physical paths, based on convenience or availability [12], limiting the mobility issues, which cause difficulties in the communication due to the short inter-contact time among vehicles and enabled a whole new set of applications.

However, the IoV paradigm has brought to many unprecedented challenges, such as how to handle the vast amount of data generated, how to find the right vehicle that can provide the right service and to which extent the information provided by other vehicles/RSUs can be trusted. Powerful applications require vehicles to collaborate by exchanging information and services, e.g., vehicles that exchange information about the traffic to find alternative routes to avoid accidents or construction works, or transport authority which mines information from the vehicles to analyze the overall city's traffic and act accordingly. In the foreseen scenarios of frequent objects interactions, it is important to understand how the information provided by some objects have to be processed so as to build a reliable system on the basis of their behavior.

The idea to use social networking notions within the IoT to allow objects to autonomously establish social relationships is recently gaining fast popularity. The driving motivation is that a social-oriented approach is expected to support the discovery, selection and composition of services and information provided by distributed objects and networks [13, 14, 15, 16]. The SIoT is intended as a social network where every node is an object capable of establishing social relationships with other things in an autonomous way with respect to the rules set by the owner. Lately, this paradigm has been extended to the vehicular context and has generated several instances of the SIoV, also called Vehicular Social Network (VSN) [17]. In the SIoV, vehicles and RSUs only need to meet in order to create their relationships; the creation of relationships has less stringent requirements w.r.t. communication, so even short range protocols not specifically designed for the IoV, such as the Wi-Fi, can be used to let the vehicles be in range of each other.

First ideas of socialization between vehicles have been introduced in [18], where the authors propose VeDi, a vehicular crowd-sourced video social network over VANETs, where users share a video with neighboring vehicles interested in such a multimedia content. In [19], the authors present S-Aframe, an agent-based multilayer framework with context-aware semantic service to support the development and deployment of context-aware applications for VSNs formed by in-vehicle or mobile devices used by drivers, passengers, and pedestrians. In [20], Yasar *et al.* show how the VSN is able to improve the information sharing in the vehicular network w.r.t. the VANET scenario and how through social relations, like Friend-Of-A-Friend (FOAF), only relevant and reliable information has to be shared between the nodes. An analytical model to measure the workloads of various subsystem involved in the SIoV process is proposed in [21] whereas the authors in [6] present an overall architecture for the SIoV, which defines the main components and their interactions; a structure of the interaction message is also proposed to support several kinds of applications for the SIoV. [22] explores the concept of the SIoV and discusses possible issues of security, privacy and trust that are likely to arise. Finally, some studies have used the social part of the SIoV to address common issues of VANET and IoV: [23] proposes a solution for content dissemination whereas [24] focused on the issue of dynamic network access. We also have presented a high-level view of the SIoV with some preliminary results [25]. A survey of the recent literature on VSNs is presented in [26].

However, all the presented papers miss a real implementation of how the social network among the vehicles can be obtained. To this, we would need data from a large number of vehicles, such as vehicle characteristics, (e.g., brand and model), mobility

Table 1: Comparison of the proposed architecture with similar approaches.

Architecture	Implementation	Simulation	Type of relations	Inter-vehicle protocols	Reference applications
Proposed implementation	Yes	-	POR, SOR, CWOR, OOR	Wi-Fi, 802.11p, BT	Vehicle Diagnostic and Smart Parking
[6]	Partially with Android devices	Partially with SUMO trace, Open Street Map and OBD2 codes	POR, SOR, CWOR, CLOR, OOR	Wi-Fi	None implemented
[19]	Yes	-	None	Wi-Fi	Smart ride application
[24]	-	Yes	POR, SOR, CWOR, CLOR	-	None implemented

tracks and the type of relationships they create with each other. This should be the first stepping stone to grasp a real understanding of the SIoV behavior. However, even if different type of relations have been foreseen, there is still no real implementation of a SIoV network. To the best of our knowledge, this is the first work that presents an implementation to create a real system where vehicles can create their own relationships, manage them and use them to query the resulting social network when looking for information and services. Table 1 compares and highlights the differences of our platform w.r.t. some of the most relevant ones available in the literature.

3. Implementation of the Social Internet of Vehicles

As explained in Section 2, the IoV scenario is a distributed system characterized by a homogeneous set of nodes with high mobility, where the vehicles can become unavailable due to the lack of connectivity as a result of the hostile propagation environment. Moreover, to support the deployment of major applications (e.g., traffic management, active road safety) and to satisfy their quality requirements, the IoV has to collect and analyze large amounts of information about the vehicles' surroundings by making the vehicles themselves cooperate with each other [27].

In such a scenario, we envision that, through the use of virtualization technologies, each vehicle/RSU in the real world is associated to its virtual counterpart in the cloud

or in the edge. Associating a digital counterpart to physical objects is a common practice in the latest IoT research activities [28], since through virtualization the physical devices are augmented in their capabilities and are able to: i) fully describe their characteristics with semantic technologies and then be able to interact with other virtual objects; ii) identify, analyze and manage the context related to an object surroundings and take decision accordingly; iii) make easy the search and discovery of services and devices, which continuously join, move and leave the network.

To enable the creation of the Social IoV, we leverage on a cloud-based platform, presented in Section 3.1, which enables to manage the social activity of vehicles as defined by the SIoV paradigm. Starting from the Social Internet of Things vision described in [29], we claim that vehicles and RSUs can create their own relationships and use these relationships to efficiently look for services and exchange information in an autonomous way for the benefit of the human user [30]. The envisioned relationships for the SIoV scenario are described in Section 3.2. Finally, in Section 3.3, we show how the major functionalities required to integrate vehicles in the SIoV could be integrated with the Intelligent Transportation System station architecture.

3.1. Cloud-based SIoV architecture

In the SIoV, the deployment of applications involves vehicles and mobile terminals (i.e., smartphones and tablets) that may move in large and complex environments together with also some static sensors (e.g., cameras and inductive coils installed at the street intersects) and RSUs, making use of solutions that have to satisfy the application quality requirements and at the same time take into account the usage of the resources not to overload some components. In this scenario, there are devices with sufficient computational capabilities, such as vehicles and RSUs, as well as devices with constraints in processing and battery, such as the sensors. It often happens that the latter devices have not the capabilities in terms of processing or battery to correctly execute the processing needed for its involvement in the running applications, as it is the case of sensors that are inquired by too many services in parallel or are asked to provide historical data exceeding the local storage capacity [31]. Additionally, it may happen the requested service does not involve the acquisition of a sensing measure in real time as it is the case of the provisioning of old data. These are the two main motivations that required the adoption of the virtualization technologies to represent the physical devices, bringing to the notion of the virtual object (VO) as a digital counterpart of any entity in the real world [28].

The VO is also the component that should take care of the establishment and management of the social links among vehicles and the other objects involved in the SIoV, bringing to the Social VO (SVO) component. The motivation to deploy these functionalities at the virtualization layer is that it can exploit the cloud / edge computing and storage capabilities that are needed to implement all the social-related functionalities. Indeed, these require to crawl the social network, evaluate the trust level of other objects and continuously analyze the context to trigger the creation of social links, among other functions. Lysis is the platform that has been developed putting at the center of the IoT the SVO and that follows entirely the SIoT model [7]. For this reason, we decided to implement the SIoV starting from this solution.
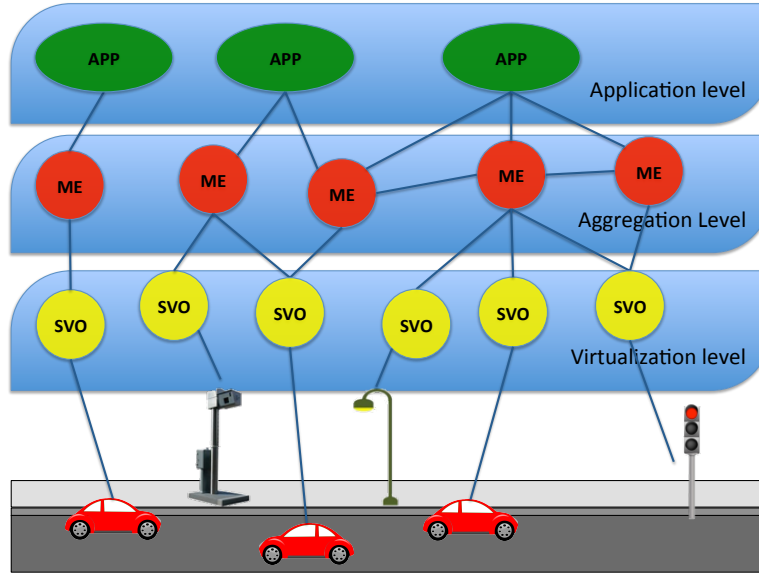
7

Figure 1: Cloud-based SIoT architectural solution.

Following the Lysis architecture, our implementation includes the following layers (see Figure 1):

- *Real World level*: this level includes the Real World Objects (RWOs), e.g., ve-
₂₄₅ hicles and RSUs, which sense the physical environment and send the acquired information to their virtual counterparts through the Internet. The hardware and software needed to turn any vehicle into a smart social vehicle compliant with the SIoV is described in Section 4.

- *Virtualization level*. The virtual counterpart of the real object is the Social Vir-
₂₅₀ tual Object (SVO), shown in Figure 2, which is equipped with two interfaces that allow for a standardized communication procedure between the aggregation level and the physical devices: the SVO-APIs enable to communicate with the aggregation level while the SVO-HAL (SVO Hardware Abstraction Layer) represents the access point with the real world and enable the establishment of a
₂₅₅ secure connection with the RWO. To differentiate among the different topologies of real entity, we create a Template, i.e., a semantic description of the related RWO, which describes its capabilities and resources. Whenever a new vehicle is registered in the platform, based on its characteristics, a SVO is instantiated according to the fittest Template. The profile, which provides a precise description
₂₆₀ of the vehicle itself, is also created during this phase, which contains a complete semantic description of the SVO instance to allow a correct search of the resources needed to create the services. Further major components in the SVO are data points, representing sensors and actuators available through REST APIs. The social behavior in the virtual objects is implemented by the Social Enabler
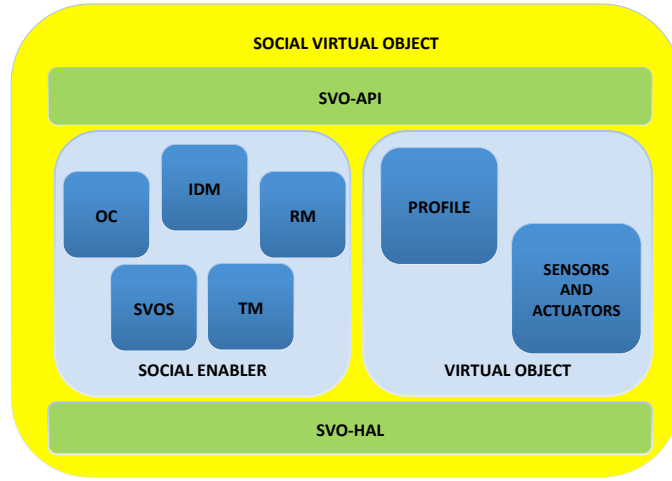
8

Figure 2: Social Virtual Object components.

(SE), which is in charge of extending the functionalities of the SVO, by adding the social capabilities to the relevant RWO. Several modules are implemented in the SE: the Owner Control (OC) allows the user to manage the rules about the establishment of relationships with other SVOs; the Identity Module (IDM) is in charge of all the operations of authentication and authorization, while the Relationship Management (RM) has the role to create, update and terminate the social relationships among vehicles, following the rules set by the owner in the OC. The resulting social graph is then used by the SVO Search (SVOS) for searching services and information requested by the application layer. Finally, the Trustworthiness Management (TM) handles the friends reputations so to build a reliable system.

- *Aggregation level*. This level aggregates data from multiple SVOs on the basis of patterns to ensure a high re-usability level. The Micro Engine (ME) is a mash-up of one or more SVOs and other MEs, which is responsible for getting and processing data from SVOs into high-level services requested by applications at the higher level.

- *Application level*. At this level, user applications are responsible for final processing and presentation. Deployment and execution of applications makes use of one or more MEs.

Each SVO interface raises a question in terms of security. When pairing a SVO with a Physical Device (PD), they exchange IDs and cryptographic keys, representing the weaker phase during which any sniffing attacks could compromise any future communications between SVO and PD. From this moment on, communication is encrypted and secure. At the application level, data can be accessed through the aggregation layer that provides an anonymous layer between users and SVOs. In the case of MEs and

9

SVOs on cloud spaces of the same provider, encrypted communication is not necessary because any security issue is within the ability to provide security from the cloud service provider. In the case of a multi-provider infrastructure or a hybrid cloud/local server scenario, security technologies related to Web applications such as asymmetric SSL/TLS encryption on HTTP/MQTT are required [32].

Some nodes can act maliciously by perpetrating discriminating attacks based on their relationships for their own gain by penalizing other parties. In addition, since the trustworthiness evaluation is integrated in the service search, the assessment of object trust is of paramount importance. Several researchers demonstrate that the social approach of the SIoT paradigm can be useful for assessing the reliability of the objects.

Although we based on an existing IoT platform, to enable the development of the SIoV we created a new Template to describe the vehicles, which can be used every time a user wants to register his/her car to the platform. Also, we developed all the software needed to enable the vehicles to communicate with its virtual counterpart, i.e., with its SVO (see Section 4.2). Moreover, we implemented the logic behind the creation of relationships among vehicles and RSUs and developed sample applications to test the resulting system. When relying on such a cloud-based IoT platform, service discovery and information exchange do not need objects to be in vicinity of each other, since they take place in the virtual world through the exploit of social relations; however, vicinity is still important to evaluate the vehicles' activity and to create such relationships.

3.2. SIoV relationships

On the basis of the SIoT paradigm, we claim that vehicles and RSUs can create their own relationships and use these relationships to efficiently look for services and exchange information in an autonomous way for the benefit of the human user. As shown in Figure 3, we identify different social interactions in the SIoV scenario:

- *Parental Object Relationship* (POR): vehicles belonging to the same automaker and originated in the same period establish a POR. This relationship can give useful information about the status of a vehicle and can be exploited when providing diagnostic services and remote maintenance to the users.

- *Social Object Relationship* (SOR): vehicles that come into contact, sporadically or continuously, through V2V communications create a SOR. Vehicles meet randomly, e.g., when their owners go to work and share the same way: more often two vehicles meet, the stronger the relationship that links each other and the higher the value it provides in service discovery and trustworthiness evaluation. The benefits given from the establishment of SORs are very important in the SIoV scenario. Indeed, most of the content provided by the vehicles are related to limited areas and to short intervals of times, as for example the communication of road incidents to vehicles proceeding toward the crashed areas or the sharing of useful information about traffic conditions or petrol stations; SORs take into account common vehicles paths and locations which permit to create social networks among vehicles strictly related to specific areas.

- *Co-Work Object Relationship* (CWOR): similarly to the SOR, when vehicles meet continuously with RSUs through V2I communications, they create a CWOR
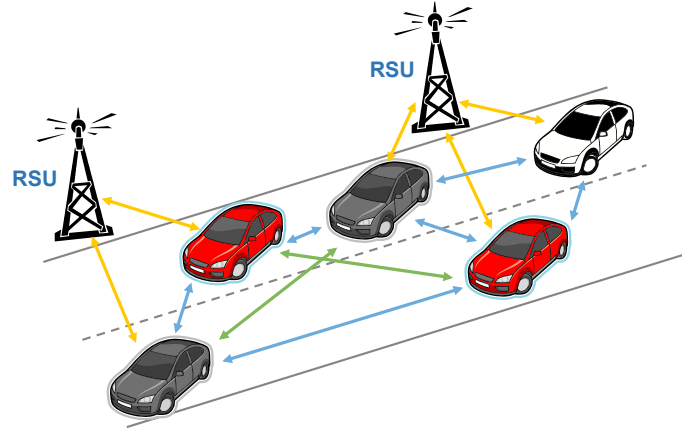
10

Figure 3: Relationships created in the Social Internet of Vehicles scenario. Green lines represent Parental Object Relationships (POR), blue lines represent Social Object Relationships (SOR) and yellow lines represent Co-Work Object Relationships (CWOR).

with them. These relationships can be useful to provide traffic information or to guide the drivers in less congestionated routes.

335 • *Ownership Object Relationship* (OOR): is defined for objects owned by the same user. For example, all the RSUs owned by the municipality are tied by this relation as well as vehicles and other objects owned by the same owner (e.g., vehicle, mobile phones, tablets).

All of the above mentioned relationships within the SIoV platform are created and 340 updated on the basis of the vehicles features (e.g., vehicle type and brand) and activities (e.g.,frequency in meeting the other objects). The combination of these relationships brings to the creation of the social network of vehicles, where information can be gathered in a distributed manner by crawling the network from friend to friend in the same way humans do in their social networks. Moreover, the SIoV evolves according to the 345 activities of vehicles and RSUs so that it can quickly adapt to the mobility scenario by creating new links or adapting the strength of the existing ones [33]. Table 2 shows some typical applications in the SIoV scenario that can benefit from the availability of social relationships between vehicles.

3.3. Integration with the ITS station architecture

350 In 1996, the National Intelligent Transportation Systems Architecture (National ITS Architecture) framework [34] has been developed, in which the Intelligent Vehicle Highway System (IHVS) services were planned and integrated, commonly known as Intelligent Transportation System (ITS)[4]. The National ITS Architecture supported the use of wireless communications for many ITS services; the SIoV concept relies on

---

[4]http://www.its.dot.gov/

11

Table 2: SIoV sample applications that can benefit from social relationships between vehicles.

Applications	Relationships	Description
Diagnostic service	POR	Vehicles contact friends to know if they have had/solved a similar issue
Traffic information	SOR	Vehicles obtain, from friends traveling along the same routes, updated information about traffic conditions
Community services	CWOR	RSUs communicate with vehicles to provide information about road conditions or maintenance

mobility technologies and cooperative communications and this type of systems are referred to as Cooperative Intelligent Transportation Systems (C-ITS). One of the most important parts of ITS systems is the ITS Station Architecture (ITS SA), which has been defined by the ISO [8] and ETSI [9] standards. In the ETSI standard, a layered description of the ITS SA is provided, which extends the horizontal OSI network layers with the vertical management and security entities. The role of the management entity is the management of communications in the ITS station whereas the security entity accounts for the provision of security to the OSI communication protocol stack. Each sub-layer is interconnected with the others via Service Access Points (SAPs) or via APIs. In [35], the ITS SA has been integrated with the 6LowPAN protocols related to the use of the IEEE 802.15.4 based access technologies to allow for the utilization of IoT standards in the ITS station. Similarly, as shown in Figure 4, we propose to integrate the ITS SA to include the middleware functionalities to allow the vehicles to be integrated in the SIoV.

The Management entity is extended with the *Device Management* and *Vehicle Control* modules. The former has the role to manage the communication between the OBU and the SVO whereas the latter handles the access to available sensors and actuators on the vehicle. The *Communication Encryption* module in the Security entity has the role to encrypt the communication between the OBU and the SVO. The *IEEE 802.15.4* and *IEEE 802.11 a/b/g/n* modules in the Access Technologies layer add respectively the ZigBee and Wi-Fi communication technologies for the OBU. The *Data Handler* module in the Facilities layer processes and converts (if needed) the data acquired by the vehicle before being sent to the SVO. Finally, in the Application layer, the *SVO Communication* application handles the communication with the SVO regarding the SIoV applications running in the cloud.

Furthermore, in the ETSI standard [9] is also provided the definition of the typical vehicle ITS station, which contains a vehicle ITS-S gateway, an ITS-S host and an ITS-S router. The ITS-S host contains as a minimum the ITS-S applications and the functionality of the ITS SA needed for the ITS-S applications. In this case, we refer to the proposed ITS SA shown in Figure 4. The ITS-S gateway interconnects an ITS station-internal network with the proprietary in-vehicle network, e.g., the Controller
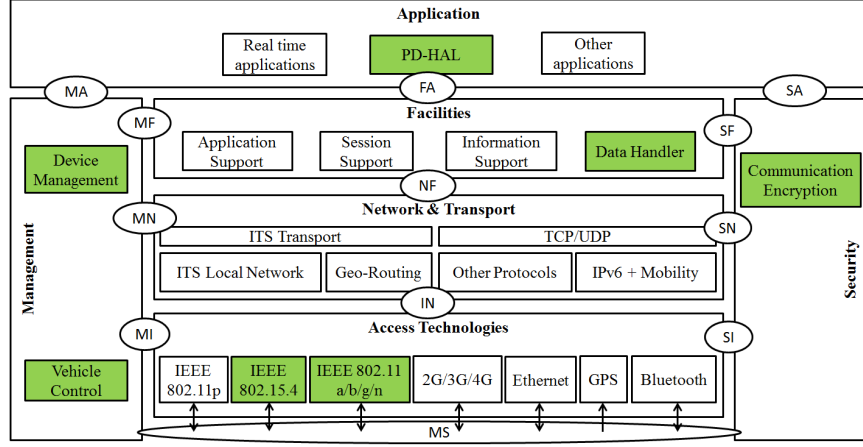
Figure 4: ITS Station Architecture integrated with the middleware functionalities to allow the vehicles to be integrated in the SIoV.

Area Network (CAN) of the vehicle. Finally, the ITS-S router interconnects the ITS station-internal network with an ITS ad hoc network or a public network [36]. The former enables ad hoc communications among vehicles, RSUs and personal ITS stations (i.e., V2V communication), whereas the latter provides mobile Internet access. In our proposal, the OBU (on which the software board runs) is the hardware device responsible for implementing the vehicle ITS station. It performs the roles of vehicle ITS-S gateway, ITS-S host and ITS-S router simultaneously. In fact, it is able to connect to the CAN through the OBD-II interface (ITS-S gateway role), it implements the functionality of the ITS SA needed for the ITS-S applications (ITS-S host role), and finally it enables V2V, V2I and Internet communication (ITS-S router role).

4. Implementation of the On-Board Unit

In this Section, we illustrate an effective low-cost and flexible solution for the OBU to enable every vehicles, even the ones without any kind of native connectivity, to participate in the SIoV and create their own relationships. In section 4.1 we discuss the implementation of the OBU hardware whereas the software modules are discussed in Section 4.2.

4.1. OBU Hardware

The followings are the hardware components and the services we have selected to build our OBU:

- *On-Board Diagnostics (OBD)*: It refers to the possibility of monitoring vehicle vital parameters for implementing self-diagnosis of the vehicle. The monitoring of vehicle parameters is done through an OBD-II connector, whose interface and pinout have been standardized by the Society of Automotive Engineers (SAE)

13

J1962 specification [37]. The OBD-II provides access to data from the Engine Control Unit (ECU), from which many vehicle parameters can be read such as vehicle speed, engine revolutions per minute, oil temperature. The OBD-II parameter identifiers (PIDs) permit to identify the vehicle parameters read from the ECU[5]. For our tests, we used an ELM327 Bluetooth OBD-II adapter, which can be connected to each device equipped with a Bluetooth interface such as a smartphone or a laptop. It costs about 10€.

- *Global Navigation Satellite System (GNSS)*: A GNSS is a system of satellites that provides autonomous geo-spatial positioning with global coverage. Currently, there are 4 GNSSs: Global Positioning System (GPS), owned by the United States; GLObal Navigation Satellite System (GLONASS), owned by the Russian Federation; BeiDou Navigation Satellite System (BDS), owned by the China; and Galileo, owned by the European Union. While the first two are fully operational, the last two are only partially operational. A GNSS is fundamental for acquiring continuously and with high precision the position of the vehicles. For our tests, we used the Telit SL869[6] module, which supports the following GNSSs: GPS L1, Galileo E1 and GLONASS L1. It costs about 15€.

- *Internet access*: Internet access is needed to enable a vehicle to communicate with its virtual counterpart. The fourth generation (4G) of wireless communication technology is the current accepted standard for mobile Internet connection, including wireless communications at vehicular speeds [38]. In 2008, the ITU-R organization specified the IMT-Advanced (International Mobile Telecommunications Advanced) requirements for 4G standards, setting peak speed requirements for 4G service at 100 Mbps for high mobility communication, such as from trains and cars. High speed communication at vehicular speeds is considered to be a key requirement for the next generation wireless broadband standard, i.e., the 5G, which is also expected to address some of the deficiencies of the IEEE 802.11p (e.g., high communication load, reliability, scalability) thanks to 5G-enabled technologies such as ProSe (Proximity Service as a Platform for Beaconing), MEC (Mobile Edge Computing) and network slicing [39]. ProSe not only provides a platform for the most desirable safety vehicular communications, but also paves the way toward determining the source of autonomous vehicle attacks. MEC promises to reduce latencies for vehicular applications that have flexible latency requirements. Network slices can be created for services such as the dedicated vehicular safety applications and emergency response applications. For implementing our OBU, we based on the 4G LTE because of its wide coverage and its capability to provide high data rates at relatively low levels of fluctuations at high vehicular speeds [38]. For our tests, we used a 4G USB dongle, which enables the connectivity to high speed 4G LTE FDD cellular networks and costs about 60€.

---

[5]https://en.wikipedia.org/wiki/OBD-II_PIDs
[6]http://www.telit.com/gnss/sl869/

Figure 5: DSRC wireless mini-PCI module (DCMA-86P2 model) from Unex.

- *Wireless short-range communication*: Wireless short-range communications take place between vehicles (V2V) or/and between vehicles and RSUs (V2I). The IEEE 802.11p standard has been specifically defined for vehicular communications in the dedicated short range communication (DSRC) spectrum [40], which offers acceptable performance for sparse network topologies and typical transmission frequencies with limited mobility support. However, the performance of 802.11p is extremely sensitive to larger vehicle densities, traffic load, and vehicle speed, which are mainly due to lack of coordinated channel access and distributed congestion control mechanisms based on in-network condition [41, 42]. Other wireless short-range protocols are IEEE 802.15.4 (ZigBee), Wi-Fi and Bluetooth (BT). ZigBee and BT are mainly used for communications in Wireless Sensor Networks and IoT whereas the Wi-Fi is the standard for wireless LAN. Therefore, these three technologies have limited applicability for V2V communication purpose as they need a longer connection time than the 802.11p and are not suitable for dynamic mobility scenarios. For example, ZigBee and BT may be used to establish V2V and V2I communications in static situations, such as between vehicles stopped at the traffic light or between vehicles facing a queue. It is important to remind that in the presented scenario, *all the information among vehicles are exchanged at the virtual level* through the use of social relationships. However, the use of short-range communications is still needed in order for the vehicles to sense the presence of other vehicles and RSUs with the aim to institute social relationships. To this aim, we considered Wi-Fi, BT and 802.11p technologies. For our tests, we used the BT 4.1 and the Wi-Fi 802.11n technologies embedded into the Raspberry Pi 3 Model B, whereas for the 802.11p technology we used the DSRC wireless mini-PCI module (DCMA-86P2 model) from Unex, which is shown in Figure 5.

- *Control board*: A control board is needed to collect all data acquired from the vehicle and to allow V2V, V2I and Internet communication. Therefore, the control board must have the needed interfaces for connecting with the OBD-II connector, the GNSS receiver and the wireless short-range module. Furthermore, it must act as a gateway, allowing the vehicle to be connected with the Internet.
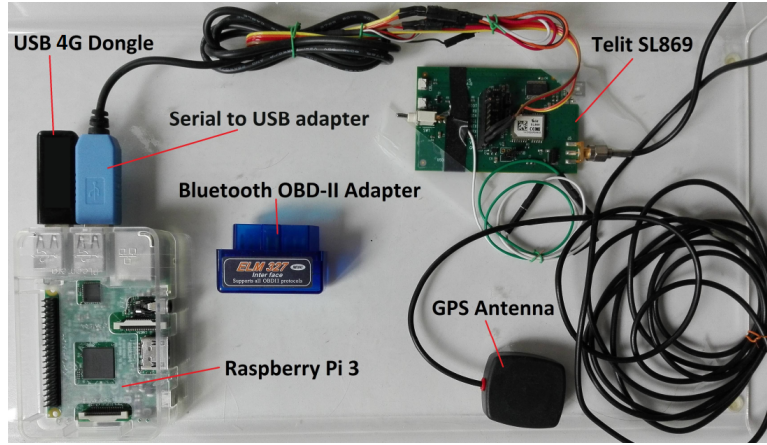
15

Figure 6: OBU implemented for our tests.

For our tests, we chose the Raspberry Pi 3 model B[7] as the control board, as it has all the requested functionalities and a low cost (about 30€).

The control board together with all the other hardware modules form the OBU, which implements all the software modules described in Section 4.2. The Raspberry has embedded BT 4.1 and Wi-Fi 802.11n technologies, which we used as wireless short-range communication interfaces for scanning the presence of close vehicles. The BT interface is also used to communicate with the BT OBD-II adapter to acquire the vehicle data. The 4G USB dongle is connected to 1 of the 4 USB interfaces of the Raspberry whereas the Telit SL869 module communicates with the Raspberry with a serial to USB adapter. The implemented OBU is shown in Figure 6 and has a total cost of about 115€.

4.2. Board Software

To communicate with the platform through the SVO-HAL, the OBU needs a software to exploit all the required functionalities: to establish a secure communication channel; to translate protocol related data values in usable value format; to implement real-time logic; and to manage the communications with several different media inside the vehicle. For this reason, the OBU implements the following modules to be part of the platform as depicted in Figure 7:

- *Physical Device-Hardware Abstraction Layer* (PD-HAL): It communicates with the corresponding module in the virtualization level. Its major role is to introduce a standardized communication procedure between the platform. It is also in charge of creating a secure point-to-point communication (encrypted) with the SVO. The pairing is done at setup phase, when the PD-HAL module exchanges IDs, URL and encryption keys with the related module in the SVO.

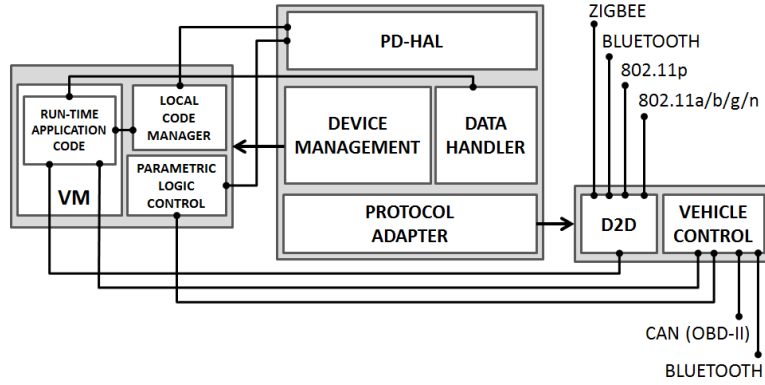[7]https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Figure 7: Software modules of the On-Board Unit.

- *Data Handler*: It intervenes whenever there is the need to process data from sensors before being sent by the PD-HAL to the virtualization level. For example, data coming from sensors could be strings of hexadecimals, which have to be processed to extract actual numerical values to encapsulate them in JSON format ready for dispatching.

- *Device Management*: It implements the actual device logic with reference to the participation of the PD to the Lysis platform, e.g., controlling the sensing frequency, managing local triggers, overseeing the energy consumption. It also runs the code that can be updated in run-time locally in the PD.

- *Protocol Adapter*: It consists in the hardware drivers to handle all local sensors and actuators.

In particular, the protocol adapter has to accomplish many of the hardware related functionalities, such as sensors/actuators vehicle management and device-to-device communications. The *Vehicle Control* (VC) module has to handle the access to available sensors and actuators on the vehicle, which in many cases, involves a cable or BT connection via OBD-II interface. The VC is also responsible for managing the connection with additional sensors on the vehicle, connected via BT, that are not managed by the ECU. The *Device-to-device* (D2D) module can handle V2V and V2I communications through several protocols such as ZigBee, BT, 802.11p and 802.11a/b/g/n. The core of the processing on the vehicle is constituted by the *Device Management* module: compared to other Lysis-enabled devices (not vehicular), this module is responsible for performing actions that require low latency or high sampling frequency from sensors or applications involving V2V and V2I communications (via the D2D module in the Protocol Adapter). The development of a huge volume of data can still be supervised by the SVO by processing statistical data, which, extracted from the application, is translated into usable format by the *Data Handler* module.

Lastly, to enable the system to update the code in run-time, we would need to use Virtual Machines to execute script interpreters (e.g., Node.js or Python), Image-based approaches, or Dynamic loadable native code components [43]. Since we do not aim

17

to manage runtime driver updates, we think that script interpreters have the right mix
between flexibility, abstraction and re-usability required by our idea of a SIoV architec-
ture. This allows us to keep the execution of part of the application code of relevance
to the device in the device itself when needed (e.g., when the application QoS require-
ments do not allow for latency levels typical of the Cloud Computing paradigm). The
source code is deployed and updated via the *Local Code Manager* (LCM) module,
which receives the source code from the PD-HAL and gives it to the interpreter. The
Parametric Logic Control (PLC) module represents the device logic which can be con-
trolled through parameters by the SVO, such as the sampling rate of the sensors, the
neighbor discovery algorithms (used as part of the process for the creation of social re-
lations between the SVO), and any IFTTT (If This Then That)-based trigger. Both the
local application and the logic control have access to the HW through the VC module
in the *Protocol Adapter* module.

5. Experimental evaluation

The objective of our experimental tests is to investigate on one of the most impor-
tant functions in the SIoV, i.e., the creation of the social relationships based on the en-
counters of vehicles. Specifically, we consider the obtainable performance when using
either Bluetooth (BT), 802.11p or Wi-Fi technologies as wireless short-range commu-
nication protocols to allow for vehicles' neighbor detection aimed at creation of social
relationships. To this, we implemented the Local Neighbor Discovery (LND) algo-
rithm presented in [44], which exploits the Wi-Fi/BT/802.11p radio interface scanning
to detect beacons transmitted by static stations. When two vehicles are able to see the
same beacon, then they are assumed to be close: after several encounters, two vehicles
become friends. This is useful in urban scenarios because of the high concentration
of Wi-Fi access points (APs). With regard to the BT and 802.11p technologies, we
investigated the performance in case of direct visibility among devices aimed at cre-
ation of social relationships. Indeed, it is unusual to find BT and 802.11p APs in urban
scenarios as well as longer scan times needed by BT for beaconing do not allow the
utilization of the LND algorithm.

The developed system was tested installing the OBU presented in Section 4.1 on
two different car models (Alfa Romeo 147 JTD and Ford Focus TDCI), which have the
same open OBD-II codes and added support to vendor specific codes of these vehicles.
We first created two instances of the vehicles on the Lysis platform, by making use
of the developed Template; then, we installed the board software on the Raspberry
and started the configuration process on the OBU that required the SVO's ID and the
car model. After configuration, the OBU set up a secure connection with its SVO, to
which the car profile description is uploaded. This information is needed to set up the
relationships among vehicles of the same model, i.e., the POR.

Each SVO collects the MAC addresses of the detected Wi-Fi APs, BT, and 802.11p
devices so that an analysis of the acquired data is possible. The LND algorithm's
behavior was tuned with five parameters: the inter-scan time (T_{is}) is the period of radio
interface scanning; the scan time (T_s) is the scan duration of the BT interface; the max
time between two detections (T_{delta}) of the same beacon for two different vehicles; the
number of the required detections (N_{fe}) for friendship establishment; the signal level

Table 3: Values of the parameters set for the tests.

| Parameter	Description	Value
T_{is}	Inter-scan time: period of radio interface scanning	10 s, 15 s, 20 s
T_s	Scan time: scan duration of the Bluetooth interface	5 s, 10 s
T_{delta}	Max time between two detections of the same beacon for two different vehicles	300 s
N_{fe}	Number of the required detections for friendship establishment	3, 6
S_{th}	Signal level threshold of the detected beacon	-90 dBm, -70 dBm, -50 dBm
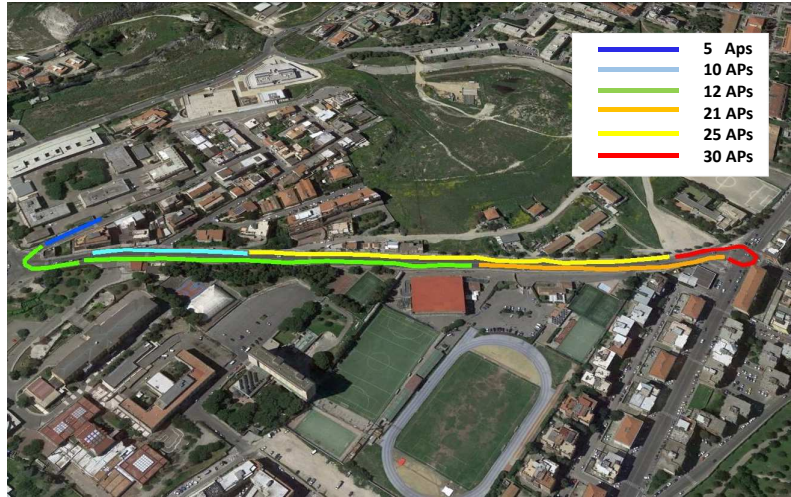
Figure 8: Access points' distribution over the testbed area.

threshold (S_{th}) of the detected beacon. In Table 3, the values of the parameters set for the tests are summarized. Figure 8 shows the detected APs in our test area by setting $S_{th} = -90$ dBm. The high diffusion of APs makes the LND algorithm suitable for our purpose.

Visibility distance: The first set of tests aimed to investigate the environmental conditions in which a new relationship is created; to this, we performed several trials
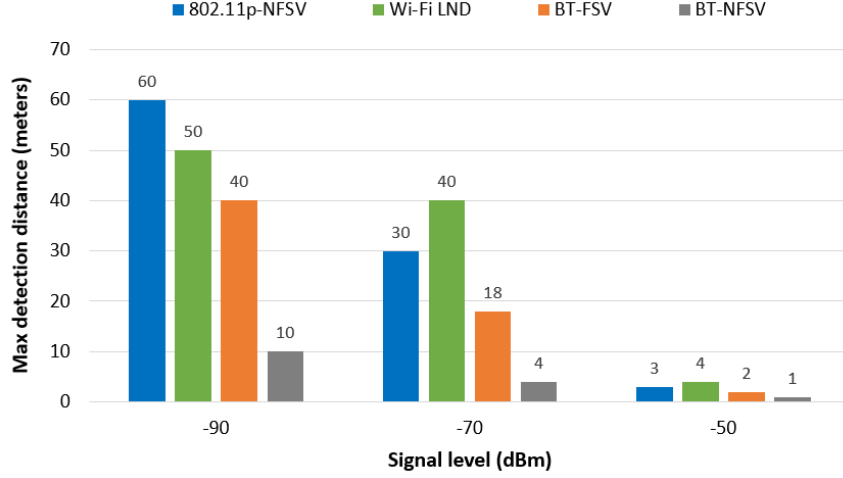
19

Figure 9: Maximum visibility distance by varying the signal level threshold: the Wi-Fi APs or other BT and 802.11p devices with an under-threshold RSSI seen by the vehicle are discarded.

to evaluate the maximum Wi-Fi, BT and 802.11p visibility distance in different situations of traffic. We only considered the visibility, regardless of direct communication availability, because visibility is the event which triggers a friendship establishment. We considered two stopped vehicles performing the LND algorithm and we conducted different tests varying the values of S_{th} to evaluate the maximum visibility (i.e., friendship) distance, as shown in Figure 9. We considered 3 different values of S_{th}, i.e., -90, -70 and -50 dBm. We measured the maximum visibility distance for 4 different cases: Wi-Fi by using the LND algorithm (Wi-Fi LND), 802.11p with other vehicles in between (802.11p-NFSV), BT in free space visibility (BT-FSV), and BT with other vehicles in between (BT-NFSV). Since it is not possible for the BT and 802.11p to use the LND algorithm for the unavailability of BT and 802.11p devices over the test area, the direct visibility has been considered.

From the results in Figure 9, as expected, the longest visibility distance decreases with the decreasing of the S_{th}, except for the 802.11p. Furthermore, the Wi-Fi LND provides the greatest values of maximum visibility distance for the greatest values of S_{th} (-50 and -70 dBm), followed respectively by the 802.11p-NSFV, BT-FSV and BT-NSFV. However, the 802.11p-NFSV provides the greatest value of maximum visibility distance for $S_{th} = -90$ dBm, followed respectively by the Wi-Fi, BT-FSV and BT-NSFV. Therefore, the Wi-Fi and 802.11p interfaces are the two technologies that are the most suitable for detecting neighbor vehicles aimed at creating social relationships in dynamic urban scenarios. Also, while the BT provides very low performance when there are other vehicles in between (BT-NFSV), it provides acceptable performance in free space when the devices are directly visible. Therefore, the BT technology may be used for static scenarios when vehicles are visible in free spaces (e.g., parking scenario).

It is important to highlight that the coverage distances reported in Figure 9 are
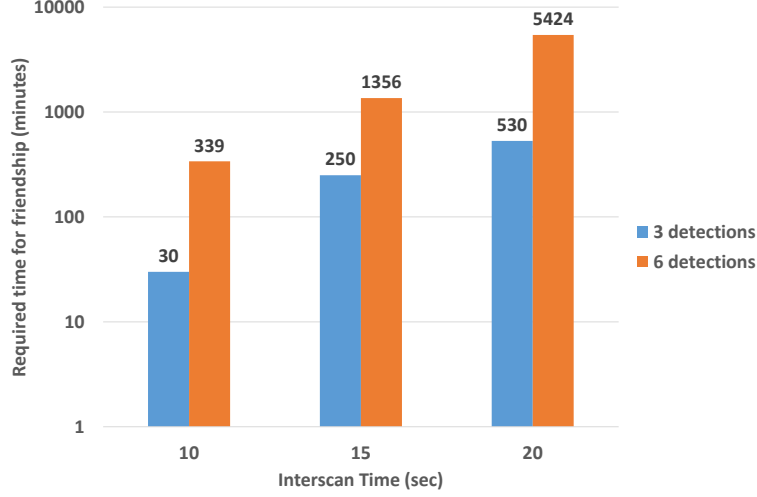
20

Figure 10: Time needed for friendship establishment by varying the values of interscan time and the number of required detections.

those maximum distances which assured the creation of the social relationship once
the considered signal level thresholds was set. This means that during the tests we
also reached visibility distances greater than 50 m with 802.11p, but these cases were
not compatible with the creation of social relationships. Indeed, to create a social
relationship vehicles must be closer enough, for example because they are travelling
along the same road or they are at the same intersection. Then, in our case, we were
not interested in creating social relationships between vehicles which are, for example,
200 m far from each other.

    Friendship establishment time: The second step of tests aimed at investigating
the time needed for friendship establishment by varying the values of interscan time
and the number of required detections. The tests have been conducted in mobility by
using the Wi-Fi LND and the results are shown in Figure 10. By setting lower inter-
scan time, it is possible to decrease the time needed to establish a social relationship
between vehicles. Indeed, it increases the possibility to find neighbor vehicles scan-
ning the same AP. Also, as expected, by increasing the number of needed detections,
the time to establish a social relationship increases. However, the number of detec-
tions is proportional to the strength of the social relationship because it means that the
vehicles are seeing each other for a long time so that they are sharing the same path.
Consequently, lower values of T_{is} provide more precision in beacons detecting. Higher
values of N_{fe} require a stronger spatial correlation in the behavior of the vehicles in
order to establish a relationship. Similarly, lower values of T_{delta} denotes a stronger
temporal correlation since the vehicles have to be close not only in space but also in
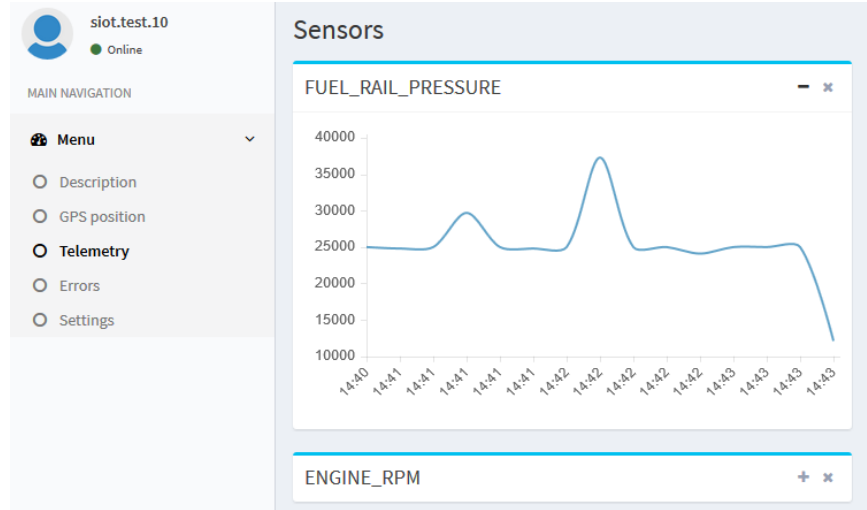time.

21

Figure 11: Telemetry view in the monitor app: charts show the sensors' values.

6. Use Cases: Vehicle Diagnostic and Smart Parking applications

In this Section, we present two sample applications that make use of the SIoV platform accessible using the proposed OBU: the Vehicle Diagnostic and the Smart Parking applications. These use-cases are meant to present the benefits of having the social relationships between our car and the others. Specifically, in the first use-case the relationships allow for presenting alerts to the other devices of the car owner for a better interaction between the user and the objects under the owner control. The second use-case shows how the social links can be used to better exchange meaningful information among friend cars, which in this example allows for easily finding the available parking lots. Due to the fact that only few real cars are currently connected to the SIoV, it is for us not possible to show performance quantitative indicators. The performance about the possibility to create the social relationships are instead shown in the previous Section 5.

6.1. Vehicle Diagnostic application

The Vehicle Diagnostic application allows the vehicle's owner to access the vehicle's data through the SIoV platform. At the first boot, the application connects to the owner's car and requires the feature list to the SVO, which replies with all the sensors and actuators accessible on the vehicle. During the initial configuration, it is possible to set the sampling frequency for data acquisition. The application enables the owner to monitor the ECU parameters and to set triggers to control the actuators via a web page available from a PC, a smartphone or from the vehicle itself if there is a display to show the application rendering. In the telemetry view, the application asks for the data log to the vehicle's SVO and shows a diagram for each numeric sensor. As an example, in Figure 11 the chart for the fuel rail pressure is shown.
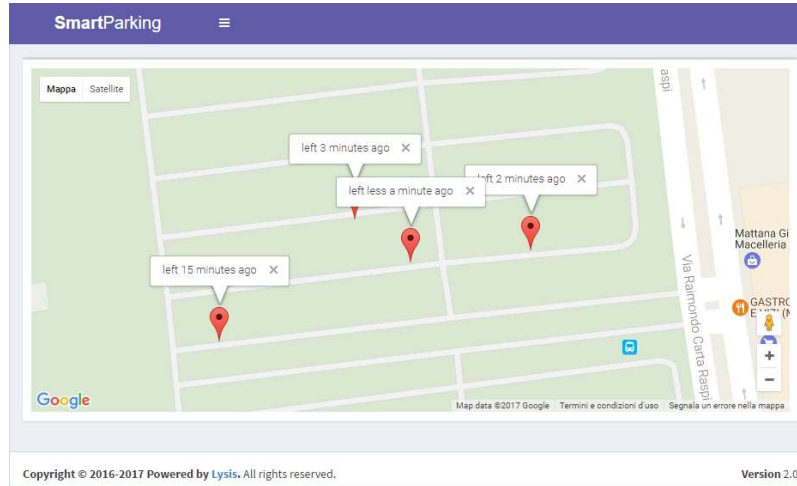
22

Figure 12: Map view in the Smart Parking app: markers show the available lots.

In the GPS position view, it is possible to see the vehicle position on the map and request for a new GPS sampling. When an error occurs, the application sends an alert to each SVO of the owner, namely to the SVOs which have an OOR with the vehicle SVO, and shows it in the Error view. Finally, in the Setting view, the car's owner can set personalized alert for each sensor on the vehicle.

Application, templates and OBU software are provided on the Lysis platform and are reusable to replicate the experiment or to use the vehicles for other scenarios.

6.2. Smart Parking application

In this scenario, we want to show how the social relationships among vehicles and parking barrier gates can be exploited to share alerts about availability of free parking lots: such alerts may be used for free parking lots along the streets, or in parking areas. We assume that the user's vehicle has already its own SVO on Lysis. Once installed, the application configures the vehicles' SVOs in order to trigger when they are leaving a free parking lot, i.e., by triggering engine turning on and velocity. In the same way, the parking barrier gate is set as well. In this case, the SVO of the leaving vehicle sends an alert with the related position to its SOR friends (vehicles and gates). Only the SVOs enabled by the application process the message so as the user can see the alerts and the free parking lot on the map as shown in Figure 12. In this way, the user can see if there are available nearby parking lots and can decide for the right direction. Since the application is a web service with web view, it can be used on a car display as well as on the smartphone/tablet.

23

7. Conclusions and lesson learnt

In this paper, we have illustrated our implementation of the Social Internet of Vehicles, which makes use of cloud and virtualization technologies. One major advantage is that the developed system is not limited to a particular technology since all the communications among the vehicles take place at a virtual level, where all the entities *speak* the same language. The resulting solution is low-cost and flexible, enabling vehicles without any kind of connectivity to participate in the SIoV. Additionally, we show how the proposed system can be integrated into the Intelligent Transportation System Station Architecture (ITS SA). The implemented system is able to collect data from the vehicle's OBU and to sense the presence of nearby vehicles. This information is then sent to an IoT platform hosted in the cloud, where friendships are created and managed on the basis of the vehicles' behavior. Through on-field tests, we have investigated on the possibility to use Bluetooth, 802.11p and Wi-Fi technologies to make vehicles detect each other and create social relationships.

From this study and relevant experiments we have acquired the following experiences:

- For the creation of the vehicles relationships there is the need to identify when two vehicles are close each other. It resulted that using the Wi-Fi interface it is possible to identify two vehicles that are close each other when their reciprocal distance is up to 50 meters. Similar performance has been achieved when using the 802.11p technology, whereas this distance is reduced to 40 meters when the Bluetooth is adopted, which further decreases to 10 meters when other vehicles are in between. Accordingly, the Wi-Fi and 802.11p are the two technologies that are the most appropriate for friendship creation.

- We found that the number of APs in an urban area in a medium size city were enough to successfully create vehicles relationships making use of the LND algorithm, i.e., two vehicles are close each other when both receive the same AP beacons. This results to be very advantageous for the SIoV as it makes more stable the creation of the friendships thanks to the fact that this does not suffer from the presence of too many vehicles in the streets that may disturb the reciprocal visibility.

- The ISO and ETSI ITS Station Architecture presents a modular framework which we have been able to follow when developing our prototype so that the proposed components can be easily integrated with systems that follow this standard architecture.

- The 802.11p technology does not introduce any major advantage in our case for the creation of social relationships as this radio technology does not allow for increasing the distance between vehicles detecting each other. However, we need to consider that it may happen that the vehicles need to send data each other directly and this is clearly easier with respect to the use of the Bluetooth and Wi-Fi case.

- Making experiments with the 802.11p technology has been quite hard as there are not many relevant products in the market, due probably by the unclear regulations in the usage of the relevant frequencies for vehicular communications. It has also been very hard to find devices with the appropriate interfaces for an easy integration in our testbed.

Acknowledgements

References

[1] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Computer networks 54 (15) (2010) 2787–2805.

[2] D. Evans, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, CISCO white paper.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular Ad Hoc network, Journal of Network and Computer Applications 37 (2014) 380–392.

[4] G. Dimitrakopoulos, Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges, in: Proc. of the 11th Int. Conf. on ITS Telecommunications (ITST), 2011, IEEE, 2011, pp. 145–151.

[5] R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, Computer 44 (9) (2011) 51–58.

[6] K. M. Alam, M. Saini, A. El Saddik, Toward Social Internet of Vehicles: Concept, Architecture, and Applications, IEEE Access 3 (2015) 343–357.

[7] R. Girau, S. Martis, A. L, Lysis: A platform for IoT distributed applications over socially connected objects, IEEE Internet of Things Journal 4 (2017) 40–51.

[8] ISO 21217:2014 Intelligent transport systems – Communications access for land mobiles (CALM) – Architecture (2014).

[9] ETSI EN 302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture (2010).

[10] H. Hartenstein, K. Laberteaux, VANET: vehicular applications and inter-networking technologies, Vol. 1, Wiley Online Library, 2010.

[11] J. Contreras, S. Zeadally, J. A. Guerrero-Ibanez, Internet of Vehicles: Architecture, Protocols, and Security, IEEE Internet of Things Journal.

[12] L. Militano, M. Nitti, L. Atzori, A. Iera, Enhancing the navigability in a social network of smart objects: A shapley-value based approach, Computer Networks 103 (2016) 1–14.

[13] A. Ortiz, D. Hussein, S. Park, S. Han, N. Crespi, The Cluster Between Internet of Things and Social Networks: Review and Research Challenges, Internet of Things Journal, IEEE 1 (3) (2014) 206–215.

[14] P. Mendes, Social-driven Internet of Connected Objects, in: Proc. of the Interconnecting Smart Objects with the Internet Workshop, 2011.

[15] E. A. Kosmatos, N. D. Tselikas, A. C. Boucouvalas, Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture, Advances in Internet of Things 1 (1) (2011) 5–12.

[16] P. Kasnesis, C. Z. Patrikakis, D. Kogias, L. Toumanidis, I. S. Venieris, Cognitive friendship and goal management for the social IoT, Computers & Electrical Engineering 57 (2017) 412–428.

[17] Z. Ning, F. Xia, N. Ullah, X. Kong, X. Hu, Vehicular Social Networks: Enabling Smart Mobility, IEEE Communications Magazine 55 (5) (2017) 49–55.

[18] K. M. Alam, M. Saini, D. T. Ahmed, A. El Saddik, VeDi: A vehicular crowd-sourced video social network for VANETs, in: Proc. of the IEEE 39th Conf. on Local Computer Networks Workshops (LCN Workshops), 2014, IEEE, 2014, pp. 738–745.

[19] X. Hu, J. Zhao, B.-C. Seet, V. Leung, T. H. Chu, H. Chan, S-Aframe: Agent-Based Multilayer Framework With Context-Aware Semantic Service for Vehicular Social Networks, IEEE Transactions on Emerging Topics in Computing 3 (1) (2015) 44–63.

[20] A.-U.-H. Yasar, N. Mahmud, D. Preuveneers, K. Luyten, K. Coninx, Y. Berbers, Where people and cars meet: social interactions to improve information sharing in large scale vehicular networks, in: Proc. of the 2010 ACM Symposium on Applied Computing, ACM, 2010, pp. 1188–1194.

[21] K. M. Alam, M. Saini, A. E. Saddik, Workload Model Based Dynamic Adaptation of Social Internet of Vehicles, Sensors 15 (9) (2015) 23262–23285.

[22] L. A. Maglaras, A. H. Al-Bayatti, Y. He, I. Wagner, H. Janicke, Social Internet of Vehicles for Smart Cities, Journal of Sensor and Actuator Networks 5 (1) (2016) 3.

[23] F. Mezghani, R. Dhaou, M. Nogueira, A.-L. Beylot, Content dissemination in vehicular social networks: taxonomy and user satisfaction, IEEE Communications Magazine 52 (12) (2014) 34–40.

[24] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, M. S. Obaidat, A Cooperative Quality-aware Service Access System for Social Internet of Vehicles, IEEE Internet of Things Journal.

26

[25] M. Nitti, R. Girau, A. Floris, L. Atzori, On adding the social dimension to the Internet of Vehicles: Friendship and middleware, in: Communications and Networking (BlackSeaCom), 2014 IEEE International Black Sea Conference on, IEEE, 2014.

[26] A. M. Vegni, V. Loscri, A Survey on Vehicular Social Networks, IEEE Communications Surveys & Tutorials 17 (4) (2015) 2397–2419.

[27] V. Pilloni, P. Navaratnam, S. Vural, L. Atzori, R. Tafazolli, Cooperative task assignment for distributed deployment of applications in wsns, in: Communications (ICC), 2013 IEEE International Conference on, IEEE, 2013, pp. 2229–2234.

[28] M. Nitti, V. Pilloni, G. Colistra, L. Atzori, The Virtual Object as a Major Element of the Internet of Things: A Survey, IEEE Communications Surveys & Tutorials 18 (2) (2015) 1228–1240.

[29] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization, Computer networks 56 (16) (2012) 3594–3608.

[30] L. Militano, M. Nitti, L. Atzori, A. Iera, Using a distributed shapley-value based approach to ensure navigability in a social network of smart objects, in: Internazional Conference on Communications, 2015, pp. 692–697.

[31] R. Kotian, G. Exarchakos, S. Stavros, A. Liotta, Impact of Transmission Power Control in multi-hop networks, Future Generation Computer Systems, In press.

[32] R. Roman, P. Najera, J. Lopez, Securing the internet of things, Computer 44 (9) (2011) 51–58.

[33] M. Nitti, L. Atzori, What the siot needs: a new caching system or new friendship selection mechanism?, in: Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, IEEE, 2015, pp. 424–429.

[34] Institute of Transportation Engineers, National ITS architecture – The concept, ITE Journal 69 (5) (1999) 9–12.

[35] L. Virágg, J. Kovács, A. Edelmayer, Extension of the ITS Station Architecture to Low-Power Pervasive Sensor Networks, in: Proc. of the 27th Int. Conf. on Advanced Information Networking and Applications Workshops (WAINA), 2013, IEEE, 2013, pp. 1386–1391.

[36] ETSI EN 302 636-3 V1.1.2 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture (2014).

[37] SAE J1962: Diagnostic Connector Equivalent to ISO/DIS 15031, Society of Automotive Engineers, https://law.resource.org/pub/us/cfr/ibr/005/sae.j1962.2002.pdf.

[38] J. Budomo, I. Ahmad, D. Habibi, E. Dines, 4G LTE-A systems at vehicular speeds: Performance evaluation, in: 2017 International Conference on Information Networking (ICOIN), 2017, pp. 321–326.

[39] S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5G for Vehicular Communications, IEEE Communications Magazine 56 (1) (2018) 111–117.

[40] J. B. Kenney, Dedicated short-range communications (DSRC) standards in the United States, Proc. of the IEEE 99 (7) (2011) 1162–1182.

[41] Z. Hameed Mir, F. Filali, LTE and IEEE 802.11p for vehicular networking: a performance evaluation, EURASIP Journal on Wireless Communications and Networking 2014 (1) (2014) 89.

[42] A. Bazzi, B. M. Masini, A. Zanella, I. Thibault, On the Performance of IEEE 802.11p and LTE-V2V for the Cooperative Awareness of Connected Vehicles, IEEE Transactions on Vehicular Technology 66 (11) (2017) 10419–10432.

[43] S. Brown, C. Sreenan, Updating software in wireless sensor networks: A survey, Dept. of Computer Science, National Univ. of Ireland, Maynooth, Tech. Rep.

[44] R. Girau, S. Martis, L. Atzori, Neighbor discovery algorithms for friendship establishment in the social internet of things, in: Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on, IEEE, 2016, pp. 165–170.

28