information

Article

A Roadside and Cloud-Based Vehicular Communications Framework for the Provision of C-ITS Services

Emanuel Vieira [1,*], João Almeida [1], Joaquim Ferreira [2], Tiago Dias [3], Ana Vieira Silva [3] and Lara Moura [3]

[1] Instituto de Telecomunicações, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[2] Instituto de Telecomunicações, Escola Superior de Tecnologia e Gestão de Águeda, Universidade de Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[3] A-to-Be Mobility Technology S.A., Lagoas Park, Ed. 15, Piso 4, 2740-267 Porto Salvo, Portugal
* Correspondence: vieira.e@ua.pt

Abstract: Road infrastructure plays a critical role in the support and development of the Cooperative Intelligent Transport Systems (C-ITS) paradigm. Roadside Units (RSUs), equipped with vehicular communication capabilities, traffic radars, cameras, and other sensors, can provide a multitude of vehicular services and enhance the cooperative perception of vehicles on the road, leading to increased road safety and traffic efficiency. Moreover, the central C-ITS system responsible for overseeing the road traffic and infrastructure, such as the RSUs, needs an efficient way of collecting and disseminating important information to road users. Warnings of accidents or other dangers, and other types of vehicular services such as Electronic Toll Collection (ETC), are examples of the types of information that the central C-ITS system is responsible for disseminating. To remedy these issues, we present the design of an implemented roadside and cloud architecture for the support of C-ITS services. With the main objectives of managing Vehicle-to-Everything (V2X) communication units and network messages of a public authority or motorway operator acting as a central C-ITS system, the proposed architecture was developed for different mobility testbeds in Portugal, under the scope of the STEROID research project and the pan-European Connected Roads (C-Roads) initiative. RSUs, equipped with ETSI ITS-G5 communications, are deployed with a cellular link or fiber optics connection for remote control and configuration. These are connected to a cloud Message Queuing Telemetry Transport (MQTT) broker where communication is based on a geographical tiling scheme, which allows the selection of the appropriate coverage areas for the dissemination of C-ITS messages. The architecture is deployed in the field, on several Portuguese motorways, where road traffic and infrastructure are monitored through a C-ITS platform with visualization and event reporting capabilities. The provided architecture is independent of the underlying communication technology and can be easily adapted in the future to support Cellular-V2X (PC5 interface) or 5G RSUs. Performance results of the deployed architecture are provided.

Keywords: cooperative intelligent transportation systems (C-ITS); roadside infrastructure; vehicular communications; ETSI ITS-G5 protocol stack

Citation: Vieira, E.; Almeida, J.; Ferreira, J.; Dias, T.; Vieira Silva, A.; Moura, L. A Roadside and Cloud-Based Vehicular Communications Framework for the Provision of C-ITS Services. *Information* **2023**, *14*, 153. https://doi.org/10.3390/info14030153

Academic Editor: Vasco N. G. J. Soares

Received: 18 January 2023
Revised: 25 February 2023
Accepted: 26 February 2023
Published: 1 March 2023

1. Introduction

C-ITS infrastructure is being deployed throughout the world with the main goals of improving travel experience, ensuring traffic safety and efficiency, and reducing environmental damage. For instance, the C-Roads initiative in Europe [1], the Connected Vehicle Pilot Deployment Program in North America [2], and the National Intelligent Connected Vehicle (Shanghai) Pilot Zone in China [3], among others, are recent examples of such endeavors. Wireless vehicular communications, also known as Vehicular-to-Everything (V2X) communications, are essential to these types of infrastructures, facilitating the exchange of information among road users, such as vehicles and pedestrians, and between them and the roadside infrastructure. The most popular contender access technologies for V2X

communications include European Telecommunications Standards Institute (ETSI) ITS-G5 based on Institute of Electrical and Electronics Engineers (IEEE) 802.11p and 3rd Generation Partnership Project (3GPP) Cellular-V2X (C-V2X), which includes both 5G Uu (cellular, long range) and PC5 (device-to-device, short range) interfaces. On the roadside infrastructure, Roadside Units (RSUs) equipped with V2X communications can also improve the perception of the overall traffic system by employing multiple sensors, such as traffic radars and cameras. These RSUs can be placed at strategic high points and critical safety locations, such as intersections and lane merges, to provide an essential view of the road state. The sensor data collected by the RSUs are processed and then disseminated to neighboring vehicles and to the road operator. This information is specially important given the nature of wireless communications, since range issues and obstacles (buildings, vehicles themselves, etc.) can negatively affect the Packet delivery Ratio (PDR), thus reducing vehicles' awareness of each other's presence on the road.

The C-ITS management platforms are the primary instrument for road operators to track all traffic information and events that take place on the roads under their supervision. Roads populated with V2X communication-enabled RSUs can inform the C-ITS platform of the position and dynamics of connected vehicles, as well as events reported by these, either automatically if the vehicle is autonomous, or manually reported through a Human–Machine Interface (HMI). Conversely, the road manager can disseminate specific warnings generated in the C-ITS platform to the areas with coverage provided by the RSUs. These warnings include accidents, roadworks, traffic jams, and other incidents. The road manager must be able to effectively handle, analyze, and extract valuable information from the vast amounts of data exchanged in vehicular networks [4]. To achieve this, the efficiency of the protocols used to distribute and collect messages in vehicular environments is critical to the design of an architecture that supports and provides C-ITS services.

Developed in the context of the STEROID—Verification and Validation of Advanced Driver-Assistance Systems (ADAS) Components for Intelligent Vehicles of the Future—research project [5] and the pan-European C-Roads initiative [1], we here present the design and implementation of a roadside and cloud architecture for the provision of C-ITS services in infrastructure-based V2X networks managed by a motorway operator (A-to-Be, the R&D company of Brisa group; https://www.brisa.pt/en/about-us/companies/a-to-be/, accessed on 25 February 2023) and a telecommunications research institute (Instituto de Telecomunicações; https://www.it.pt/, accessed on 25 February 2023) in Portugal.

The rest of the paper is organized as follows. Section 2 provides a description of the related work in the area. In Section 3, the roadside infrastructure and cloud architecture are presented, followed by Section 4 describing where the roadside equipment is effectively deployed. To complement this work, on-field performance test results of the devised and installed architecture were performed, according to the materials and methods Section 5, being the obtained results presented in Section 6. To conclude the paper, Section 7 provides a discussion and future work.

2. Related Work

Work related with C-ITS architectures includes not only academic papers, but also full pilot projects, demonstrating the feasibility and advantages of C-ITS services.

Du et al. [6] describe a distributed message delivery infrastructure designed for connected vehicles that consists of three layers. The first layer is responsible for collecting data from connected vehicles, the second layer is responsible for distributing the data to appropriate recipients, and the third layer consists of applications that use the infrastructure to provide services to end-users. The architecture uses Apache Kafka, a fault-tolerant, multi-worker data stream processing platform that provides a publish/subscribe messaging model. Data collected from vehicles are published to Kafka topics, which are then subscribed to by the message delivery layer for efficient and scalable message delivery. Kafka's support for partitioning and replication is noted as a good fit for the infrastructure, as it allows for horizontal scaling and provides fault-tolerance and high availability. Overall,

the proposed infrastructure provides a reliable and scalable messaging system to handle the large volumes of data generated by connected vehicles.

Hugo et al. [7] propose a C-ITS architecture focusing on the flow of data between the central traffic management system and the vehicles, and among the vehicles themselves. Apache Kafka, with its distributed message processing capabilities, and the MQTT protocol, a publish–subscribe messaging protocol, serve as the bridges between the vehicular system entities. A Kafka cluster is used for the processing of ITS messages, such as encoding and decoding, and it is connected to both the central traffic management system and a MQTT broker. The MQTT broker forwards the messages between the vehicles and the Kafka cluster. This way the road manager, operating the central traffic management system, can transmit and receive messages to and from the vehicular network composed of the vehicles. To analyze the performance of the system a machine was used to run the Kafka cluster and simulated vehicles, and an external Microsoft Azure machine was used to run the MQTT broker. Cooperative Awareness Messages (CAMs), which are the beacon-like messages of the ETSI ITS vehicular systems, are used to generate traffic in the setup. However, as mentioned by the authors, both the Kafka cluster and simulated vehicles are running on the same machine, which negatively affects the performance and invalidates a fair analysis of the system, the results show the feasibility of the proposed architecture and small overhead of the Kafka-based mechanism. In [8], the same authors propose a SUMO (Simulation of Urban Mobility) and veins-based vehicular simulation framework to test the same designed C-ITS architecture.

Lu et al. [9] propose a broker-centric architecture for the geographical-based exchange of C-ITS messages. Here, vehicles, RSUs, and other users subscribe and publish messages to one or several MQTT topics. Each topic is associated with a defined area or region, calculated using a successive division of the Earth in four quadrants. This system allows for a user to easily disseminate information to several Intelligent Transport System Stations (ITS-Ss), i.e., the vehicles and RSUs, located in a specific region, at once. The authors also provide a short description of a JSON Web Token (JWT)-based mechanism for user authorization, to enhance the security of the provision of broker-based C-ITS services. Other works employ MQTT and this geographical tile topic approach, including [7,10], and the framework proposed in this paper. Our own approach based on this system for the exchange of information between the roadside and cloud infrastructure is described in more detail in Section 3.

RSU placement is also a critical aspect in the design of infrastructure-based vehicular networks aiming to provide the best possible coverage. This is especially important in urban scenarios, where the presence of buildings and other urban infrastructure can severely degrade the quality of communications among vehicles. Gozalvez et al. [11] measured how buildings, bridges/terrain elevation, trees and vegetation, roundabouts, and traffic, influence the performance of 802.11p-based vehicular communications, and showed that these are heavily influenced by the environment. The authors also provide guidelines for the deployment of RSUs. These include placing RSU antennas high when trees/vegetation are not present and placing them low if trees/vegetation are present. Placing the RSU antennas high can also be advantageous in scenarios with high traffic density and in the presence of heavy vehicles (trucks, buses, etc.). Laha et al. [12] aim to optimize the RSU locations in urban scenarios in order to ensure maximum network coverage while minimizing the number of RSUs required and the associated deployment cost. Using simulations, the authors show that the proposed approach is more cost-efficient when compared to a greedy approach.

The large scale deployment of C-ITS infrastructure and traffic management systems is largely boosted by research projects and public–private initiatives. Some examples include SCOOP@F (Système Coopératif Pilote at France) [13], InterCor (Interoperable Corridors) [14], CONCORDA (Connected Corridor for Driving Automation) [15], NordicWay [16], and C-MobILE (Accelerating C-ITS Mobility Innovation and depLoyment in Europe) [17], among others. To provide service continuity for vehicles in cross-border

scenarios, some deployments, such as the InterCor project, span multiple countries. These deployments include the installation of RSUs for direct communication with vehicles and the associated backhauling network interconnection. This project addresses the interconnection and interoperability issues of several international C-ITS European corridors. The vehicular networks of roads in the Netherlands, France, Belgium, and the United Kingdom are interconnected. A communication network architecture is defined for this purpose, where the interface between the roadside system and the vehicle is established using ETSI ITS-G5. An additional interface for the exchange information of between the roadside system and the back-office system is also included in the architecture.

In some pilots, such as the PASMO (Open Platform for the development and experimentation of Mobility Solutions) project [18], a myriad of road sensors is deployed, including RSUs, traffic radars, Internet Protocol (IP) cameras, parking sensors, and weather stations, whose operations depend on different protocols. In such a scenario, a cloud software platform based on the Machine-to-Machine (M2M) paradigm must handle high device heterogeneity using diverse communication protocols, such as Hypertext Transfer Protocol (HTTP), MQTT, Constrained Application Protocol (CoAP), and Advanced Message Queuing Protocol (AMQP), among others. Moreover, these systems must also handle various communication technologies for data collection and information exchange, such as ITS-G5, Long Term Evolution (LTE), Long Range (LoRa), radio links, fiber optics, etc., increasing the integration complexity of all components.

Strobl et al. [19] provide the design of a C-ITS (Cooperative Intelligent Transport Systems) architecture that was implemented in a pilot project in Dresden, Germany, as part of the "Synchrone Mobilitat 2023" initiative. The architecture comprises three main components: vehicles, RSUs, and cloud-side infrastructure. The cloud-side infrastructure provides centralized backend services that facilitate data exchange between all entities using the MQTT protocol. The RSUs and the backend services, such as the traffic monitoring system, are designed to be highly modular. This means that they consist of several independent software modules, each running in Docker containers. The modular design provides flexibility, scalability, and ease of maintenance, as each module can be updated or replaced without affecting the rest of the system.

Scalable cloud solutions are required to manage the enormous and heterogeneous amounts of data generated by road traffic systems, including standard ETSI C-ITS messages, such as CAM, Decentralized Environmental Notification Message (DENM), Infrastructure to Vehicle Information Message (IVIM), Signal Phase and Timing Extended Message (SPATEM), Collective Perception Message (CPM), and more, as well as other types of information, such as Local Dynamic Maps (LDMs), High Definition Maps (HD-Maps), raw sensor data, video streams, among many others. Geocasting techniques, such as the ones implemented in the C-MobILE project [17], simplify the process of linking all road users, including vehicles, service providers, and traffic management centers (central C-ITS stations). These techniques are based on the same MQTT geographical tiling scheme mentioned earlier.

Connected and Automated Vehicles (CAVs) can rely on additional sources of data for extending their fields of view and having more detailed information about their surrounding environment. This is made possible by the C-ITS infrastructure, incorporating devices ranging from roadside sensors and communication units to cloud C-ITS components. As a result, CAVs can make more informed decisions or even delegate some of those decisions to the roadside or cloud infrastructure, optimizing traffic speed and safety features. The AUTOPILOT (automated driving progressed by Internet Of Things) project [20] is an example of such a deployment, as it uses the IoT ecosystem to integrate connected cars and transform them into automated moving objects. It also uses interoperable M2M platforms to connect all parts of the traffic system.

Recently, other communication technologies have been tested to deliver C-ITS services even in challenging environments, such as cross-border regions [21]. These Cooperative, Connected and Automated Mobility (CCAM) applications are expected to benefit from

the next generation of mobile networks (5G), providing high reliability and availability, high bandwidth, and low end-to-end latency. Therefore, it is critical to plan and create a roadside and cloud architecture that is independent of the underlying communication systems used to exchange data among the many traffic agents.

3. Roadside and Cloud Architecture

A vehicular communications framework was developed as part of the design and implementation of mobility testbeds in Portugal, namely those deployed under the scope of STEROID research project [5] and A-to-Be's participation in the pan-European C-Roads initiative [22]. This framework consists of a roadside and cloud architecture to support C-ITS services along some of the nation's motorways. The main objective of this architecture is to support road safety use cases in networks of vehicles with infrastructure assistance. Figure 1 presents a representation of the developed and implemented architecture.

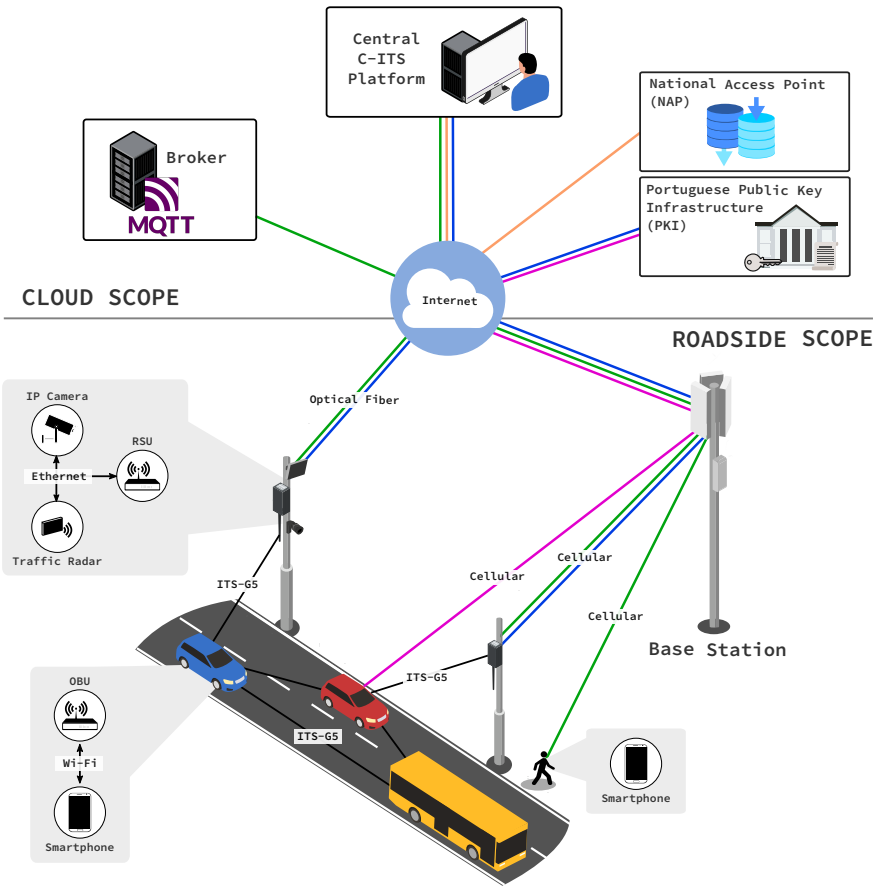

Figure 1. Roadside and cloud-based C-ITS architecture.

The roadside infrastructure consists of ITS-G5 RSUs connected to the backhauling network by fiber optics or cellular (3G/4G/5G) networks. To provide the C-ITS framework with more information, such as the presence and dynamics of legacy (i.e., non-connected) vehicles or Vulnerable Road Users (VRUs) on the road, some additional road sensors are attached to the RSUs, such as traffic radars and IP cameras.

A cloud-based MQTT Broker, used by all RSUs, facilitates information exchange and connects them to the central C-ITS Platform (MOBICS—Mobility Intelligent Cooperative Systems [23]). This platform enables the handling of all data exchanges between C-ITS devices, the current road infrastructure, and the road operator's traffic control technologies. For example, it enables the continuous monitoring of all road activity. It allows a human operator to signal a traffic event, such as roadworks or traffic accidents, at a specific geographical location, triggering the C-ITS platform to generate the corresponding C-ITS

message automatically. This C-ITS message is typically either a DENM in the case of specific events, or an IVIM in the case of advisory or mandatory contextual speed limits or road signage information. This message is then delivered to the relevant location served by the local RSUs.

Additionally, the C-ITS Platform is continually connected to the National Access Point (NAP) for the exchange of high-level transport-related data in DATEX-II format and to the Portuguese Public Key Infrastructure (PKI) for the implementation of the security measures outlined in ETSI standards. The management of certificates and credentials between the Root Certificate Authority, the Enrolment Authority, and the Authorization Authority in the PKI and the RSUs and the On-Board Units (OBUs) on the road is made possible by this PKI interconnection.

All the entities of the roadside and cloud frameworks are described in more detail below, focusing on the main entities that act as a bridge between the local vehicular network and the road manager, that is, the RSU and the cloud MQTT broker.

3.1. Roadside Architecture

The roadside architecture consists of the roadside infrastructure and, by extent, by all road users which are able to communicate with it. We can identify three types of entities, namely, RSUs, connected vehicles with OBUs, and VRUs.

3.1.1. Roadside Unit (RSU)

RSUs provide support to the vehicles circulating on the road and are typically stationed close to it. They act as a bridge between the local vehicular network and the road managers responsible for managing and monitoring the roads. They can disseminate and retransmit important vehicular data and events for improved information dissemination. For the devised architecture, a roadside unit (Figure 2), was developed in partnership between A-to-Be Mobility Technology S.A. and Instituto de Telecomunicações, comprised of a Single Board Computer (SBC) connected to a VERA V2X series ITS-G5 board from u-blox [24]. A Global Navigation Satellite System (GNSS) receiver for positioning and time synchronization is included. In addition, an embedded LTE module or optical fiber-based link provides connectivity to the Internet and, by extent, to the cloud infrastructure from which the road manager can manage the RSUs. The road operator interacts with the RSUs either through a Secure Shell Protocol (SSH) connection used for RSU setup, configuration and maintenance, or through an MQTT-based approach specifically for vehicular data exchange, which is detailed in the following subsection.

Figure 2. A deployed RSU. It is pictured: the front of the RSU (**top left**) with frontal power switch and USB, Ethernet and HDMI ports; the back of the RSU (**bottom left**) with back power switch, power socket and GSM/LTE, DSRC (ITS-G5) and GNSS antenna connectors; and the housing of the RSU adjacent to a motorway (**right**).

A multilayered Open Systems Interconnection (OSI)-like architecture characterizes the current software implementation of the ITS-G5 RSUs. Five vertical services and two parallel services compose the architecture. Each layer is associated with a running service (C program) where Interprocess Communications (IPC) are established through the ZeroMQ networking library. Figure 3 represents the implemented ETSI ITS-G5 protocol stack.

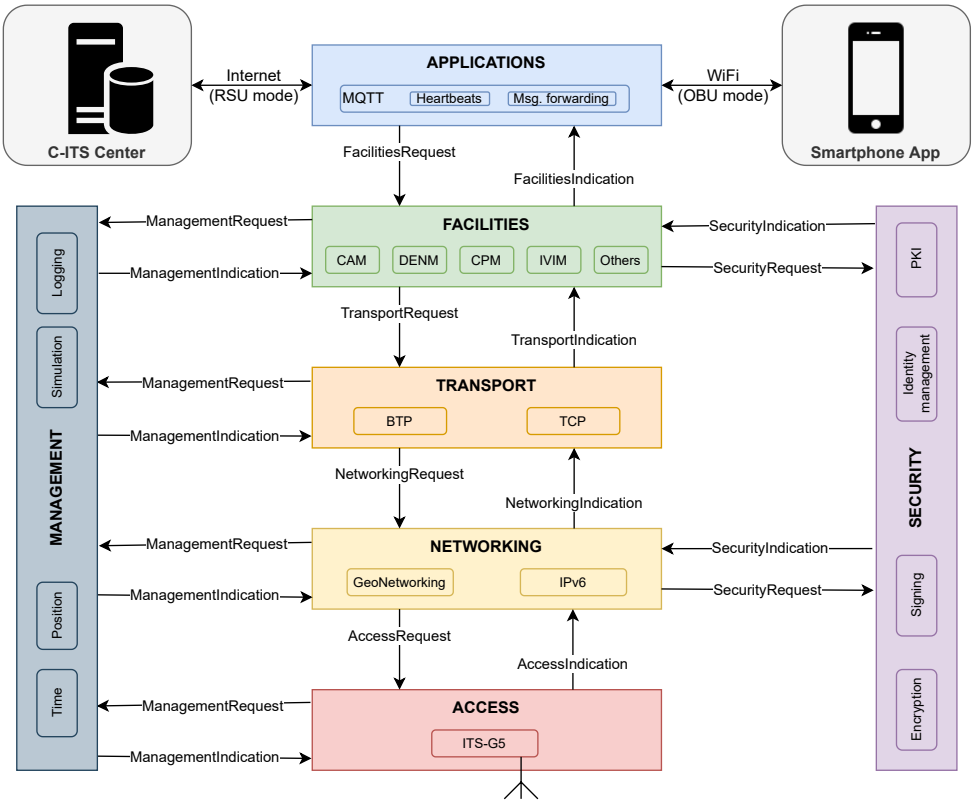

Figure 3. Implemented ETSI ITS-G5 protocol stack.

- The Access service, is responsible for managing the access technologies and encapsulating and decapsulating the packets' Ethernet protocol headers, namely the Media Access Control (MAC) [25], and Logical Link Control (LLC) [26,27] headers. This service serves as the bridge between the physical layer and the rest of the upper stack, handling the transmission and receiving of packets;
- The Networking service, which mainly implements the GeoNetworking (GN) [28] protocol, is a geographical addressing and packet forwarding system for point-to-point and point-to-multipoint communications. This service also implements the IPv6 protocol [29], and the GN/IPv6 adaptation sublayer (GN6ASL) [30] to combine IPv6 and GN routing features. GeoNetworking and IPv6 packet header encapsulation and decapsulation procedures are handled here;
- The Transport service, which implements the Basic Transport Protocol (BTP) [31], a transport layer protocol similar to User Datagram Protocol (UDP) [32], and the Transmission Control Protocol (TCP) protocol [33]. BTP provides port numbers to address upper-layer sub-services and is similar to UDP in that it does not provide a reliable connection between devices like TCP. The Transport service is responsible for processing the BTP and TCP headers.
- The Facilities service supports various ETSI ITS standard-defined sub-services. The current implementation provides support for the processing of beacon-like CAMs [34] through the Cooperative Awareness (CA) subservice, event-focused DENMs [35] through the Decentralized Environmental Notification (DEN) subservice, IVIMs [36] through the V2I oriented Infrastructure to Vehicle (IVI) subservice, radar-based CPMs [37] through the Collective Perception (CP) subservice, and non-safety Services

Announcement Essential Messages (SAEMs) [38] through the Services Announcement (SA) subservice;

- The Security service aims to provide and verify the authenticity in the vehicular network and manage the trust among ITS-Ss. It is responsible for creating signatures and verifying them carried on the packet's GeoNetworking Secured Header and triggering identity change across layers for privacy purposes. The identity change is a process where services simultaneously change identifiable information, such as GeoNetworking address, a certificate in use, and station ID. The goal is to increase user privacy through rotational pseudonymity, making the tracking of the vehicle by onlookers more difficult.
- The Management service provides several kinds of information for the remainder of the protocol stack. It provides the ITS-S with time and position, and record packets sent back and forth between layers for applicational purposes. It can also simulate both time and position depending on how it is configured; for example, in OBU mode, the ITS-S can simulate its position to follow a specified route;
- The Applications service is a standard agnostic implementation supporting specific applications and ITS-S interactions. Employed applications include forwarding ITS messages from the ITS-G5 environment to the cloud system, vice-versa, and a heartbeat system, both implemented using an MQTT approach.

In the IPC implemented among the services, Service Data Units (SDUs) are exchanged through ZeroMQ. The format of these SDUs follows defined structures using the Abstract Syntax Notation One (ASN.1) description language, which aims at providing future service interoperability and ease of code development. Exchanged SDUs are encoded following the Octet Encoding Rules (OER).

By using ZeroMQ, the protocol stack can run and easily switch between different distributed modes. For example, each service can run on a different machine over ZeroMQ's TCP. This can prove to be helpful as the ITS-S can outsource to a higher performing machine any service except the Access service, e.g., outsource the Facilities service where radar data for CPM generation may need to be processed constantly, or outsource the Security service to a more central and secure server for key and credential storage. However, one must consider the additional latency associated with this scheme, as interprocess communications are typically faster than communications over a network.

Broadcasted messages are signed and verified at the Networking layer using requests to the Security service, which specializes in key and certificate management. Security is implemented as defined per the standards ETSI TS 103 097 [39], and ETSI TS 102 941 [40], where the former is based on the IEEE WAVE 1609.2 security standard [41]. Signatures are based on the Elliptic Curve Digital Signature Algorithm (ECDSA) and are either 256-bit or 384-bit. These signatures are created using private keys, whose corresponding public keys are included in temporary certificates known as Authorization Tickets (ATs) that are shared between the ITS-Ss. Tickets are issued by an Authorization Authority, which is included in the Portuguese C-ITS PKI and, by extension, included in the European C-ITS PKI.

An RSU can also be equipped with traffic radars and cameras, which can significantly increase its perception. Some radars can discretely identify road objects (vehicles, VRUs) and classify them according to their volume, lessening the computational load on the RSU by feeding it this already processed information. Data from these types of sensors can be processed locally by the RSU and then disseminated in the form of CPMs, which contain information about the sensed objects' dimensions, position, and speed. Disseminated CPMs provide valuable information to connected vehicles about legacy vehicles and other road users without V2X capability. Moreover, CPMs containing information about connected vehicles are also valuable to other connected vehicles, as factors such as range limitations, environmental obstacles, or packet loss issues can reduce perception among them (mainly provided through CAM dissemination). Connected vehicles with these sensors can also share their collected data through CPMs. In the implemented design, some RSUs are equipped with smartmicro's traffic radars [42]. The connections between them

are established by short Ethernet cables, which are used by the RSU to connect via a local IP to fetch the sensed objects' processed and classified radar data. RSUs with IP cameras do not currently establish a direct connection with them, although they are connected to the same local Ethernet network. The IP camera feed is streamed over the Internet to the C-ITS platform.

3.1.2. Vehicle and On-Board Unit (OBU)

Any type of road vehicle with an OBU providing vehicular communications, is able to exchange vehicular information in the architecture. This includes, private vehicles, such as cars, motorcycles and trucks, as well as public entities and authorities, such as public buses, police vehicles, and other emergency vehicles. A cellular module providing access to the Internet is usually included in the OBU for PKI-related certificate operations or other applicational purposes. A Wi-Fi module can also be included to provide Internet to the vehicle's passengers. The described protocol stack used by the RSU is also employed by the OBU.

To assist the driver with the vehicular information exchanged in the vehicular network, a smartphone application was developed [43] in the current architecture to act as an HMI. The application is continuously connected to the OBU through the Wi-Fi connection provided by the latter. Information is exchanged through the MQTT protocol, where the broker (server) runs locally on the OBU. Messages received by the OBU (CAMs, DENMs, CPMs, etc.) are forwarded to the broker where they are published. The application, subscribed to the respective topics, fetches these messages and provides a viewable translation of the message data, such as the positions of perceived objects in a CPM or the event position and type in a DENM. A driver can also create events in the application that are associated with DENMs, such as accidents or roadworks. These generated events are published in the OBU's broker and then forwarded and broadcast through ITS-G5 to neighboring ITS-Ss.

3.1.3. Vulnerable Road User (VRU)

Road users who do not typically use motorized vehicles, such as pedestrians and cyclists are classified as VRUs. Their safety can be enhanced through the use of position sharing devices or HMIs.

The developed application described above can also function in VRU mode, where the smartphone is connected to the cloud MQTT broker through a cellular connection. The user's position is continuously published to the broker and all nearby subscribed data (CAMs, DENMs, CPMs, etc.) are viewable in the application. In OBU mode, the user can also disseminate events published in the cloud broker. The road manager can then act on this information and transmit it to RSUs near the event to be broadcast by ITS-G5 to connected vehicles. Apart from the user's position, no identifiable information is shared.

Snapshots of the application can be seen in Figure 4. A view of an RSU disseminating CPMs with perceived vehicles (in blue) and a list of the possible warnings that can be generated by the smartphone user are shown. The Android application can be downloaded via Google's Play Store (CCAM App. https://play.google.com/store/apps/details?id=com.it2s.it2smobileapp, accessed on 25 February 2023).

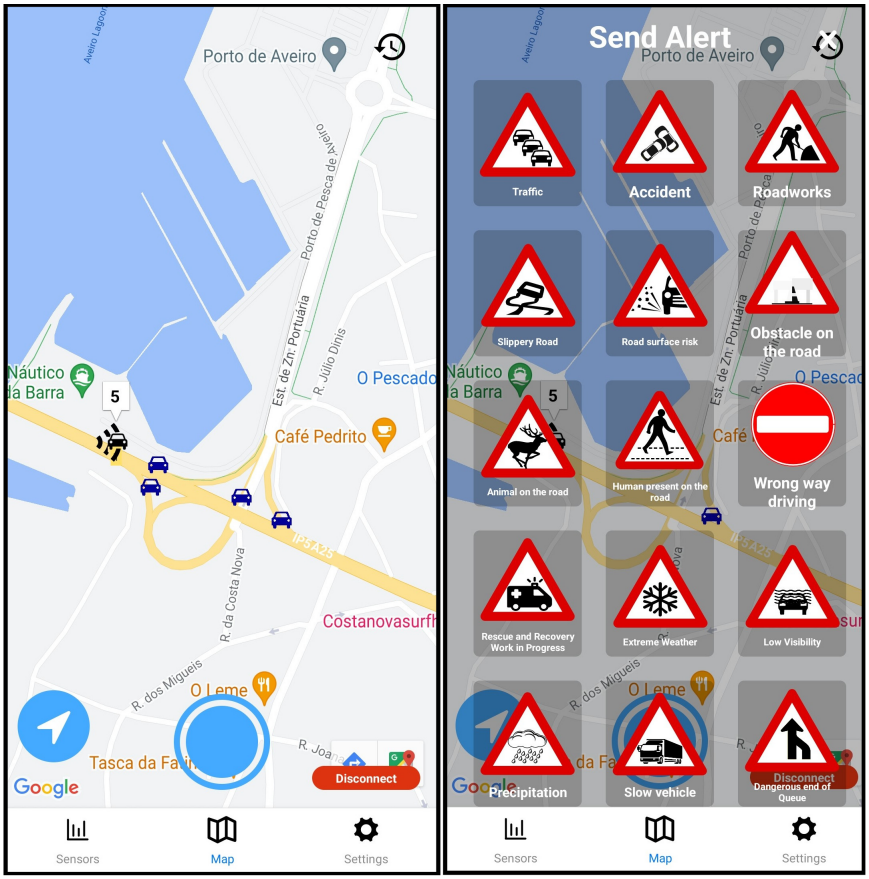

Figure 4. CCAM application: visualization of an RSU transmitting CPMs (**left**); and the alert (DENM) generation panel for the user to disseminate warnings (**right**).

3.2. Cloud Architecture

The cloud architecture provides support to the roadside architecture by helping to disseminate of important information such as accidents through alerts, and by enabling security and trust in the vehicular network through the public-key infrastructure. Four entities compose the cloudside architecture, namely, the cloud MQTT broker, the central C-ITS platform (MOBICS, road manager), the Public Key Infrastructure (PKI) Certificate Authorities (CAs), and the National Access Point (NAP).

3.2.1. Cloud MQTT Broker

In safety-critical systems such as vehicular systems, the efficiency of information dissemination and reception is critical. The road manager must be able to inform the local vehicular networks of possible events as quickly as possible, and receive information from them, process it, and possibly retransmit it in an efficient manner. To do this, the road manager must have an effective way of managing the data transmitted across all of its RSUs. The communication protocol used for communications between the RSUs and the central C-ITS platform (operated by the road manager) must be chosen specifically accounting for several required features, namely,

- Security: RSUs/central C-ITS platform must be able to authenticate themselves and privately transmit data (through encryption);
- Reliability: no transmitted messages should be lost in the connection between RSU/-central C-ITS platform;
- Communication patterns: the road manager must be able to inform and receive information from multiple RSUs as efficiently as possible;
- Performance: the communication technology should be as efficient and lightweight as possible, given the embedded nature of the RSU hardware.

A comparison between popular application layer communication protocols, namely HTTP, MQTT, CoAP, and AMQP, is presented in Table 1. Security-wise, all protocols except CoAP employ Transport Layer Security (TLS) as the encryption and authentication protocol. AMQP also provides the option of using Simple Authentication and Security Layer (SASL). CoAP, being based on UDP, employs instead Datagram TLS (DTLS). Reliability-wise, all protocols except CoAP work on top of the TCP, where CoAP uses UDP. Given TCP's native retransmission and required acknowledgments, this protocol ensures the reception of transmitted packets, whereas UDP does not provide such features. Patterns-wise, the publish/subscribe (PUB/SUB) model is preferable to a request/response (REQ/REP) approach since the former allows for one to transmit the same information to several nodes at once (e.g., transmit accident information to several RSUs at once). Both MQTT and AMQP support PUB/SUB, whereas HTTP and CoAP do not. Performance-wise, both MQTT and CoAP were developed for the Internet of Things (IoT) with an embedded hardware focus, while also possessing smaller overheads (header length) in the exchanged messages. Considering the mentioned features and the provided the comparison, MQTT was chosen as the communication protocol to be used.

Table 1. Comparison between several application layer protocols.

Feature	HTTP	MQTT	CoAP	AMQP
Encryption	✓(TLS)	✓(TLS)	✓(DTLS)	✓(TLS or SASL)
Authentication	✓(TLS)	✓(TLS)	✓(DTLS)	✓(TLS or SASL)
Reliability	✓(TCP)	✓(TCP)	✗(UDP)	✓(TCP)
REQ/REP pattern	✓	✗	✓	✓
PUB/SUB pattern	✗	✓	✗	✓
Embedded/IoT focus	✗	✓	✓	✗
Header length	Variable (min. 26 bytes)	Variable (min. 2 bytes)	Variable (min. 4 bytes)	Variable (min. 8 bytes)

A persistent cloud MQTT broker implemented using the Mosquitto library is used as a communication bridge between the RSUs (running an MQTT client) and the central C-ITS platform (MOBICS). ITS messages received by the RSU through ITS-G5 are forwarded to the central C-ITS platform through MQTT. ITS messages, such as the manually triggered DENMs and IVIMs, can also be injected into the ITS-G5 environment by specific RSUs chosen using an MQTT geographical-based topic system based on [9]. The topic used system has follows the structure described in Listing 1.

Listing 1. MQTT topic system used for RSU-MOBICS ITS message exchanges.

```
its_center/[QT]/[MF]/[ID]/[MT]/[LOC]
```

Here, `QT` is the message destination (inqueuefor messages published by the RSUs or outqueue for messages published by MOBICS), `MT` is the message encoding type (e.g., binary or Extensible Markup Language—XML), `ID` is the ITS-S identifier number, `MT` is the type of ITS message (e.g., CAM, DENM, or IVIM), and `LOC` is the current location of the RSU following a quadtree map system representation.

In this representation, each Earth quadrant is represented by a digit from 0 to 3, where the quadrant 0 represents northwest, 1 represents northeast, 2 represents southwest, and 3 represents northwest. Each quadrant can be divided into four quadrants following the same logic, this being performed in succession until a desired zoom/resolution level is reached.

For example, an RSU stationed at (+46.989482, +8.866957) (World Geodetic System 84) with a station ID equal to 5642 that would receive a Unaligned Packed Encoding Rules (UPER)-encoded DENM from the ITS-G5 environment could encode it as XML (currently,

the only message format used in the implemented MQTT system) and would publish it under the topic indicated in Listing 2.

Listing 2. Example MQTT topic to which an RSU with station ID 5642 stationed at (+46.989482, +8.866957) would publish a DENM.

```
its_center/inqueue/xml/5642/DENM/1/2/0/2/2/1/3/0/0/1/0/0
```

In this case, the system uses a quadtree of zoom level equal to 12. RSUs are also subscribed to various topics which the MOBICS platform can use to disseminate messages. An RSU is subscribed to the outqueue instead of the inqueue, to the station ID equal to 1 (used as the identifier for MOBICS platform), to all types of C-ITS messages, and to all quadtree zoom levels, from level 1 to a predefined level, z_{max}. For example, the same RSU as in the previous example, and for $z_{max} = 14$, it would subscribe to the topics indicated in Listing 3.

Listing 3. Tile-based MQTT topics to which an RSU stationed at (+46.989482, +8.866957) would subscribe. The wildcard "+" means that the RSU subscribes to all ITS messages.

```
its_center/outqueue/xml/1/+
its_center/outqueue/xml/1/+/1
its_center/outqueue/xml/1/+/1/2
...
its_center/outqueue/xml/1/+/1/2/0/2/2/1/3/0/0/1/0/0
its_center/outqueue/xml/1/+/1/2/0/2/2/1/3/0/0/1/0/0/3
its_center/outqueue/xml/1/+/1/2/0/2/2/1/3/0/0/1/0/0/3/3
```

The RSU also subscribes to all messages directed only to itself, as indicated in Listing 4.

Listing 4. ID-based MQTT topic to which an RSU with station ID 5642 would subscribe. The wildcard "#" means that the RSU subscribes to all ITS messages published to any location.

```
its_center/outqueue/xml/5642/#
```

Following these schemas, the road manager can choose to publish messages affecting one or several regions by using a combination of topics with different quadtrees and zoom levels and can also choose to publish messages only to a specific RSU. MQTT security is implemented using TLS certificates. Additionally, the RSU implements a heartbeat mechanism that periodically publishes its current status to the MQTT broker. These heartbeat messages contain summarized information, including current CPU and memory usage, current IP address, and active C-ITS events within its coverage area.

3.2.2. Central C-ITS Platform

All messages from the ITS-G5 environment, including periodic messages such as CAMs and event-driven messages such as DENMs and IVIMs, along with the current status of each RSU in the field, can be viewed on a dashboard provided by the road manager's main tool for overseeing and monitoring traffic, the central C-ITS platform (MOBICS). Figure 5 presents snapshots of the MOBICS dashboard. Through its graphical user interface, MOBICS also enables the user-friendly production of traffic events. This makes it easy to monitor all traffic activity and disseminate C-ITS warnings as necessary.

The central C-ITS platform functions as a traditional traffic management system, but with V2X features for to communicate with road devices (RSUs and OBUs) and advanced road sensors, such as traffic radars and cameras. A traffic management operator can use it to filter received messages and monitor the condition of RSUs, while also setting rules for events to be generated automatically or manually.

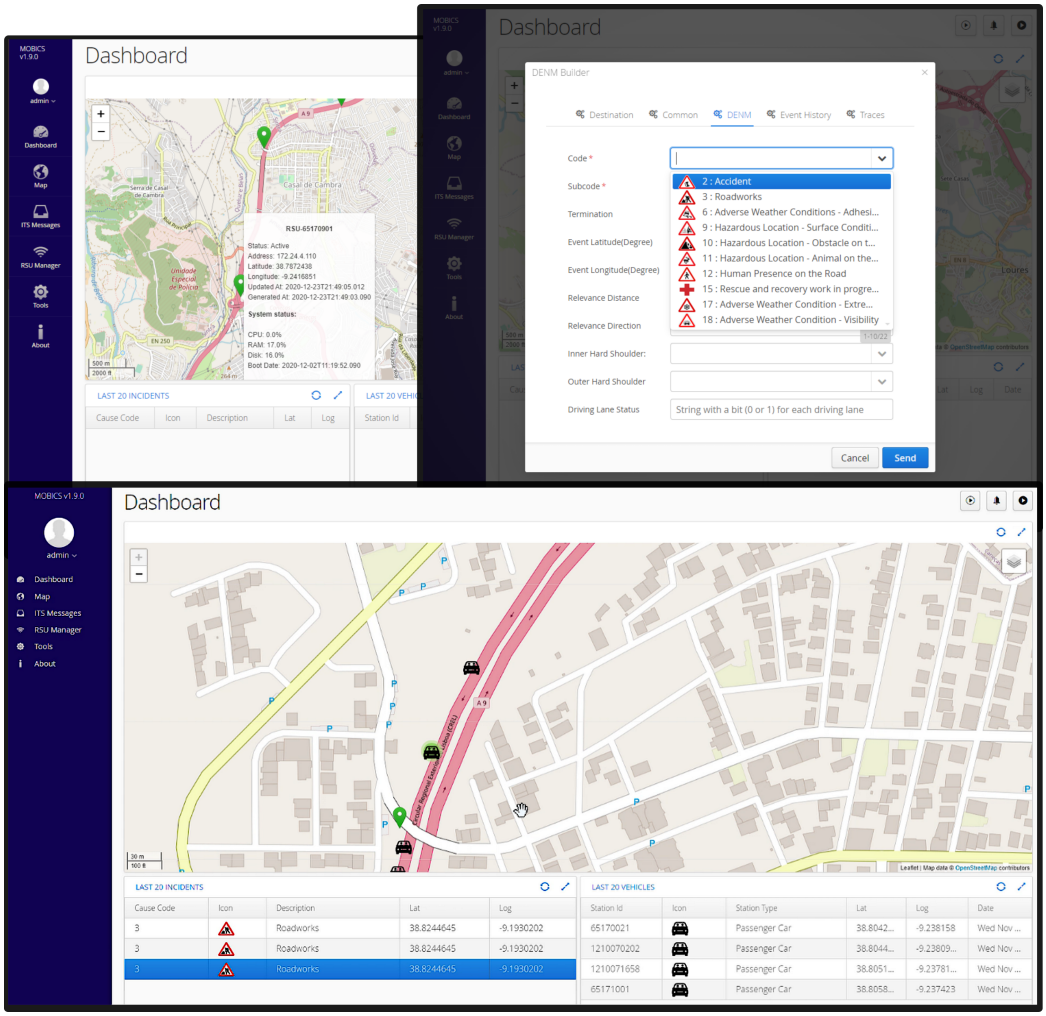

Figure 5. MOBICS dashboard interface, version 1.9.0 (current). Features include, the monitoring of RSUs statuses (**top left**), generation of events (**top right**), and traffic and history overview (**bottom**).

MOBICS adopts an open architecture that makes possible cooperation with other central systems (with the aim of eliminating human intervention) or with an access point (e.g., NAP) for the exchange of information, e.g., regarding traffic events. Currently, the platform is able to interpret CAM, DENM, and IVIM messages received or sent to the cloud MQTT broker, but it is planned to extend it include more ETSI ITS message types, such as VRU Awareness Message (VAM), Maneuver Coordination Message (MCM), Map (lane topology) Extended Message (MAPEM), and SPATEM. In the future, ASN.1 encoded ITS messages in binary format will also be supported, not only XML as at present. In terms of hardware, both the central platform and the cloud broker can be run on the same machine or on their own separate dedicated servers.

3.2.3. PKI's Certificate Authorities (CAs)

The PKI plays a key role in providing security and trust between the road users composing the local vehicular network. ITS-Ss, such as the vehicles' OBUs and RSUs, employ temporary and rotatory certificates—the Authorization Tickets (ATs)—which grant them both privacy and authentication in the vehicular network. Trusted authorities, namely, the certificate authorities (CAs), are responsible for providing the root of trust in the vehicular system, issuing ATs to requesting ITS-Ss.

Requesting certificates from CAs is typically an automatic process, where new certificates are requested when currently owned certificates start to reach the end of their validity period. In the designed architecture, the road manager can also manually upload

CA-issued certificates to a deployed RSU through the available SSH connection. Other changes to the PKI, such as changes to the CA certificates themselves, can also be uploaded to the RSUs via this connection.

3.2.4. National Access Point (NAP)

As part of a European Commission initiative to improve the interoperability of mobility-related services and facilitate the travel experience in the European Union, each member state should have a NAP to which users and road operators can connect to exchange transport-related data and/or metadata. Access to data is provided in a non-discriminatory basis, and related implementations must follow standards defined by the European Commission. NAPs can also provide Application Programming Interfaces (APIs) for programmatic data exchange.

In the designed architecture, a NAP serves as a bridge between the various road managers to exchange traffic-related data. Through the central C-ITS platform, the road manager can disseminate NAP-originated events, such as accidents, to the road users through the devices connected to the cloud MQTT broker, such as RSUs and user smartphones (through the designed application). User-generated events can also be published in the NAP, after due verification by the road manager.

4. Deployment Scenario

The presented C-ITS infrastructure in this paper is being deployed along several motorways in Portugal, covering the region around the capital city of Lisbon and some areas close to the borders with Spain, in order to also test cross-border interoperability aspects. The locations of the RSUs already installed by A-to-Be are depicted in blue in Figure 6, as well as the corridors covered in the Portuguese C-Roads project. Other RSU sites are also being deployed by distinct project partners managing different motorways in the country (markers in orange).

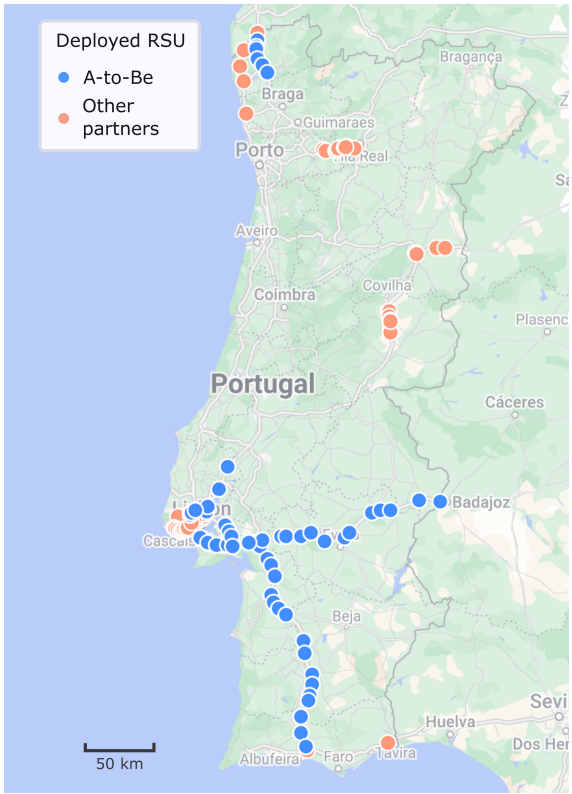

Figure 6. Deployment scenario of the C-ITS infrastructure in Portugal. Each dot corresponds to a deployed RSU.

The project tested "Day 1" and "Day 1.5" services over a length of 460 km of roads, focusing mostly on Infrastructure-to-Vehicle (I2V) pilot use cases, namely Vehicle Data Collection, Animal or person on the road, Weather Condition Warning, Stationary vehicle, Traffic Jam Ahead, Emergency Vehicle Approaching, Accident Zone, Lane closure, Dynamic Speed Limit Information, and Embedded Variable Message Sign (VMS) "Free Text".

The same designed architecture was also implemented in the scope of STEROID project covering Aveiro region in central Portugal. Figure 7 presents an overview of the installed RSUs and the C-ITS platform application. Green squares represent the installed RSUs, while the blue circles represent the perceived objects (vehicles) by the RSUs with traffic radars. The coverage areas include a motorway and an urban environment. The present deployment serves as a testbed for vehicular services.

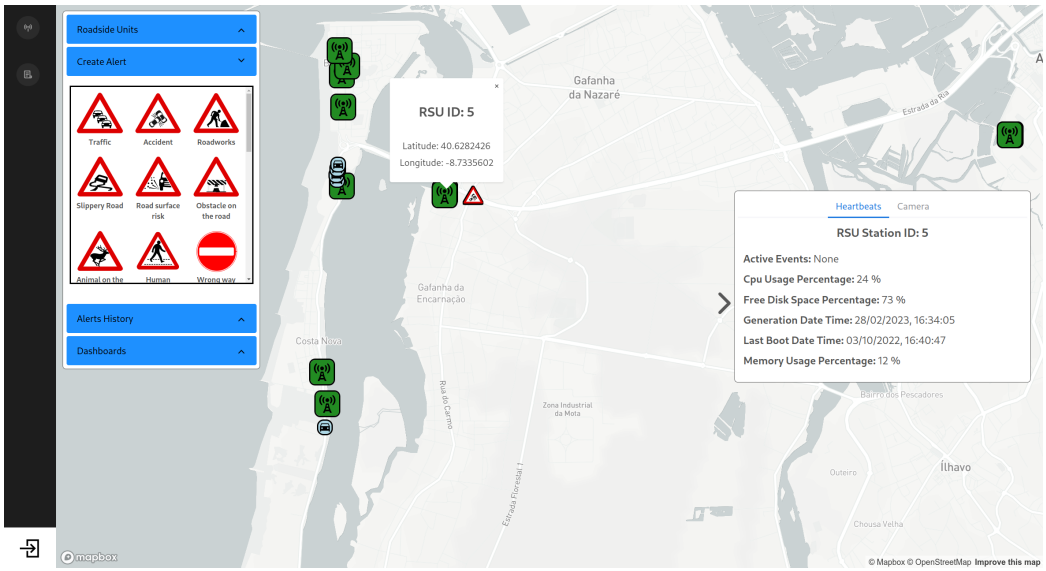

Figure 7. Overview of the STEROID deployment scenario and C-ITS platform. RSUs statuses and nearby traffic perceived by the RSUs radars can be viewed. The C-ITS platform can also generate events and forward them to respective RSUs.

5. Materials and Methods

To analyze the performance of the system, on-field tests were performed using an OBU, an RSU and the cloud MQTT broker. While the OBU communicates only with the RSU through ITS-G5 using broadcast messages and vice versa, the RSU also communicates with the cloud MQTT broker using either fiber optics or LTE. The latency of the time taken for messages generated in an OBU to reach an application, such as the central C-ITS platform, connected to the cloud MQTT broker is analyzed.

The OBU employs the same ITS-G5 protocol stack used by the RSUs as described in Section 3.1, running on Arch Linux while the cloud MQTT broker runs an Eclipse Mosquitto instance also on top of a Arch Linux virtual machine with 4 cores and 16 GB RAM. PC Engines APU3 boards are used as the ITS-S hardware, consisting of an AMD GX-412TC 4-core CPU @ 1200 MHz and 4GB RAM. Any cryptographic operations carried out by the protocol stack are performed by this CPU.

Time synchronization is achieved using the Network Time Protocol (NTP) for the cloud broker, which uses an NTP server in the same network, achieving sub-millisecond accuracy. For the OBU and RSU, the Precision Time Protocol (PTP) is used instead, where a dedicated Raspberry Pi is employed as a time server, obtaining current time information through a GNSS receiver's Pulse-Per-Second (PPS) signal. The connection between the OBU/RSU and the Raspberry Pi is established using a small Ethernet cable, achieving sub-microsecond accuracy. A visualization of an RSU identical to the one used in the tests is provided in Figure 8.

Packets, their timestamps and other associated metadata are recorded in the ITS-S in the Facilities and Access services, and in the cloud broker server, where a lightweight C Mosquitto program functioning as a MQTT client is constantly listening and recording all ITS messages arriving at the broker. Data were recorded and stored using three MariaDB instances, one running in the OBU, one running in the RSU and one running in the cloud broker server.

In the presented tests and results only CAM packets were transmitted. The generation rate of CAMs was set at 10 Hz using a static OBU. As per the ETSI ITS standards, CAMs are generated at the Facilities service, then forwarded to the Transport service to be encapsulated with the BTP protocol headers, then sent to the Networking service to be encapsulated with the GeoNetworking protocol headers and optionally sent to the Security service to be signed, and lastly forwarded to the Access service to be encapsulated with the LLC and MAC headers so that the message can be broadcasted through ITS-G5. Received messages follow the opposite path, being decapsulated by the responsible services and the signature verified by the Security service. Received messages are also forwarded by the Facilities service to the Applications service, where they are forwarded again to the cloud broker through MQTT.

Figure 8. An RSU used for performance analysis of the proposed implemented system. It is connected via Ethernet to a Raspberry Pi which functions as a timeserver. The pair of larger antennas are used for ITS-G5 communications, while the pair of smaller antennas are used for LTE communications.

Access-wise, the ITS-G5 Control Channel (CCH) was used to transmit these messages on the 5.9 GHz frequency at 23 dBM power, with a default data rate of 6 Mbit/s. A distance of 35 m separated the OBU and RSU. Since ITS-G5 has a high PDR up to several hundreds of meters [10,44] (varying according to transmission power, vehicle speed, and obstacles, among others factors), we expect the packet loss rate to remain extremely low to non-existent at 35 m. An installed on-field RSU with a fiber optics and an LTE connections provided by a commercial operator was used for the tests. The RSU is connected to a private VPN, providing access to the same network as the cloud broker. The RSU was first connected to the Internet via fiber optics and then by LTE. A representation of the described test setup is presented in Figure 9.

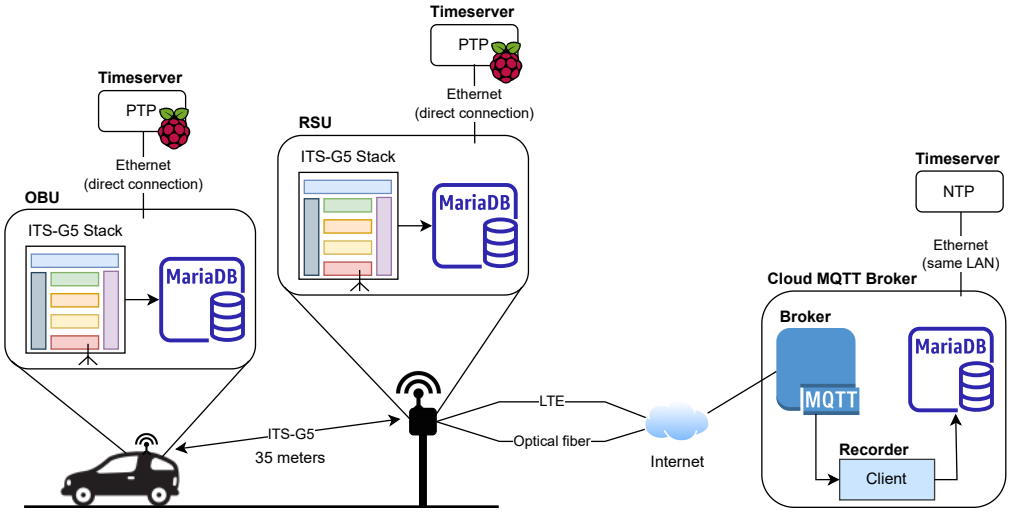

Figure 9. Setup used for performance measurements. A stationed vehicle continuously broadcasts CAMs through ITS-G5 which are then forwarded by an RSU to the cloud MQTT broker. A lightweight client in the broker server records the received messages.

6. Results

The latencies measured between the OBU, RSU, and cloud MQTT broker using the setup described in the previous section, are presented below. Only the packet flow latencies from the OBU to the RSU and then to the cloud broker were measured to analyze the delays between the three different entities. All results are provided in milliseconds. A PDR of 99.91% was measured for the OBU-RSU ITS-G5 connection and 100% of the messages were successfully transmitted in the RSU-Broker LTE/fiber MQTT-based communication.

The fiber optics connection-based results are presented in Table 2 and Figure 10. A sample size of 10000 transmitted CAMs is represented. The results show a lower latency between RSU and broker (10.32 ms) compared to the latency between OBU and RSU (17.49 ms), but with a higher variance. It is also worth noting that the OBU-RSU connection includes more processing and analysis of the exchanged packets across the several services, in particular more computing power is required for the computation of the cryptographic procedures by the Security service.

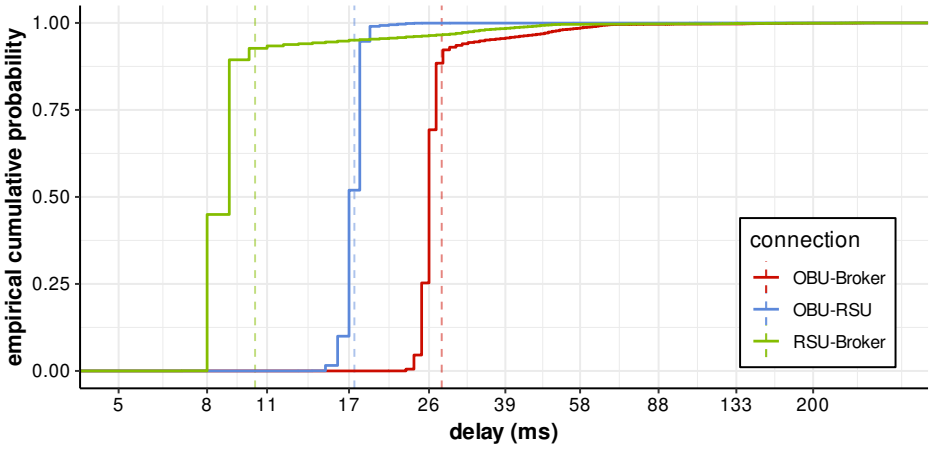

Figure 10. Empirical CDF representation of the OBU (Facilities layer) to RSU (Facilities layer) to cloud broker (listening client) message delay with the RSU with a fiber optics connection to the Internet. The vertical dashed lines represent average values.

Table 2. OBU (Facilities layer) to RSU (Facilities layer) to cloud broker (listening client) delay results in milliseconds for with the RSU with a fiber optics connection to the Internet.

	Mean	Std. Dev.	Min.	Max.
OBU-RSU	17.49	2.45	13	164
RSU-Broker	10.32	11.15	7	337
OBU-Broker	27.81	11.45	21	355

Overall, the time that took for a CAM to reach an application using the cloud broker since it was generated was on average 27.81 ms, with a minimum delay of 21 ms and a maximum delay of 355 ms.

The LTE connection-based results are presented in Table 3 and Figure 11. A sample size of 10000 transmitted CAMs is represented. Results show a noticeable increase in the delay (76.05 ms on average) compared to the fiber optics results (10.32 ms on average). The variance of the measured delays is also much higher, with a standard deviation of 325.32 ms versus 11.45 ms and a maximum of 4574 ms versus 355 ms.

Table 3. OBU (Facilities layer) to RSU (Facilities layer) to cloud broker (listening client) delay results in milliseconds for the RSU with an LTE connection to the Internet.

	Mean	Std. Dev.	Min.	Max.
OBU-RSU	17.45	1.19	13	92
RSU-Broker	76.05	325.32	21	4574
OBU-Broker	93.50	325.36	38	4592

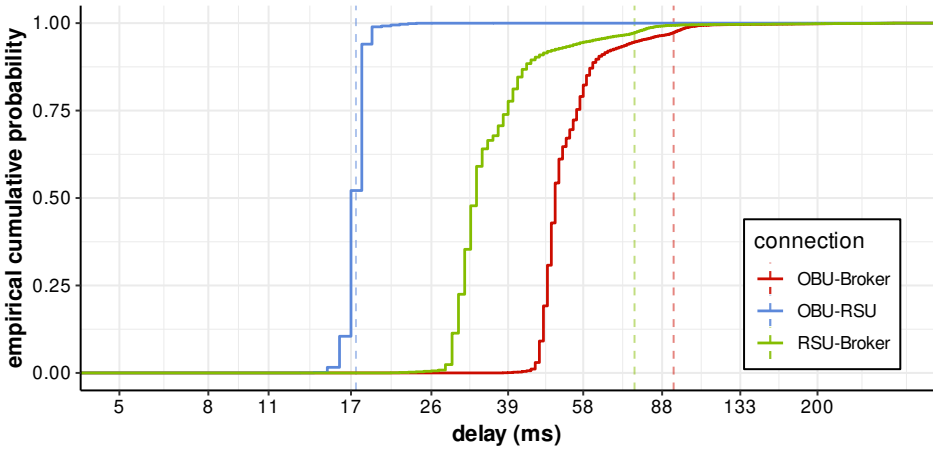

Figure 11. Empirical CDF representation of the OBU (Facilities layer) to RSU (Facilities layer) to cloud broker (listening client) message delay with the RSU with an LTE connection to the Internet. The vertical dashed lines represent average values.

Overall, the time that took for a CAM to reach the cloud MQTT broker since it was generated was on average 93.5 ms with a minimum delay of 38 ms and maximum delay of 4592 ms. Comparing to a fiber optics connection, it should be preferred over an LTE one, specially for more time sensitive applications. This is only if fiber optic connectivity to the Internet is available at the spot of the RSU installation.

As expected, the type of RSU connectivity to the Internet does not affect the performance of the OBU-RSU ITS-G5 communications, as the average delay remains about the same, 17.45 and 17.49 ms. These results include the processing of the CAM packets performed by both the protocol stacks of the OBU and RSU.

The average packet size transmitted is 533 bytes. This includes the CAM message payload, BTP header, GeoNetworking headers, message signature and occasionally associated certificate, and LLC and MAC headers.

Results recorded at the Access layer, where no associated packet processing takes place, are presented in Table 4 and Figure 12. A sample size of 10,000 transmitted CAM packets is represented.

Table 4. OBU (Access layer) to RSU (Access layer) delay results in milliseconds for packets with no processing associated.

	Mean	**Std. Dev.**	**Min.**	**Max.**
OBU-RSU	2.1	0.51	1	9

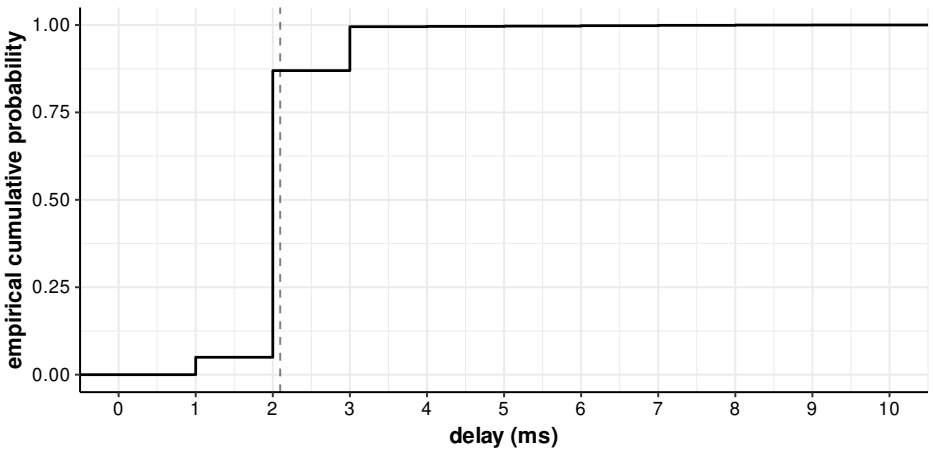

Figure 12. Empirical CDF representation of the OBU (Access layer) to RSU (Access layer) message delay. Sample size of 10,000 CAMs. The average values is indicated through the vertical line (2.1 ms).

Results show an average of 2.1 ms for a CAM packet to be transmitted between two ITS-Ss. The difference between the Access layer and Facilities layer results (17.47 ms) can be pointed to the packet processing as mentioned earlier. Moreover, the use of ZeroMQ in the ITS-S protocol stack also incurs an added latency every time the services exchange SDUs with each other. Results for the ZeroMQ IPC performance is provided in Table 5.

Table 5. ZeroMQ interprocess communication delay in milliseconds. A sample size of 10,000 requests of 500 bytes each.

	Mean	**Std. Dev.**	**Min.**	**Max.**
ZeroMQ IPC	0.383	0.054	0.213	1.579

Given that it takes approximately 0.383 milliseconds to transmit a message between services, ZeroMQ IPC communications contribute on average $0.383 * 4 * 2 = 3.064$ ms (four message exchanges in the OBU and four message exchanges in the RSU) to the total delay between the OBU and the RSU stations at the Facilities layer.

7. Conclusions

Cooperative, Connected and Automated Mobility (CCAM) requires the design and implementation of reliable, scalable, and interoperable C-ITS infrastructure that combines both roadside equipment with cloud components, services, and platforms. The paper summarizes the roadside and cloud architecture devised for the deployment of C-ITS use cases under the scope of STEROID research project and the pan-European C-Roads

initiative in Portugal. This work focuses on the role of the roadside infrastructure and I2V communications in CCAM applications. An analysis using on-field performance test results of the devised architecture is provided. The obtained results prove the feasibility of the proposed architecture, showing that low end-to-end delays with small standard deviation values can be attained when the back-hauling communications between the RSUs and the cloud MQTT broker is implemented over a fiber optics connection to the Internet. On the other hand, when LTE cellular networks are employed for the exchange of data with the cloud system, higher average values are obtained, and, especially critical for real-time safety applications, large standard deviation and maximum delay values are observed. The performance of the implemented ETSI ITS-G5 protocol stack on both OBUs and RSUs devices was also evaluated by measuring the delay of a packet crossing the different layers of the communications stack. These measurements have also demonstrated the lightweightness of the developed solution.

As future work, more tests with the deployed architecture will be performed, namely to study the reverse packet flow from the cloud MQTT broker to the OBU, which is an important metric considering the possibility of event dissemination by the C-ITS platform. Another important aspect to be taken into consideration is the scalability of the proposed architecture. Currently, all backhauling communications between the roadside infrastructure and the cloud C-ITS platform are centralized in a single MQTT broker. This solution performs well for a small to medium number of RSUs managed by the platform, but when many more units are deployed in the field, alternative strategies may need to be considered (e.g., hierarchical or distributed approaches, such as the introduction of Kafka clusters for enhanced message processing) to meet the pre-defined system requirements in terms of latency, availability and response time. Moreover, the impact of the security mechanism on the total delay will also be analyzed in order to understand if the use of specialized hardware for cryptographic processing could have a significant benefit. Finally, and taking advantage of the deployed cross-border corridors with Spain, interoperability tests with foreign partners will be carried out with the goal of testing standard-compliance aspects. In addition, latency measurements will also be evaluated for the OBUs crossing both countries, moving from the Portuguese PKI to the Spanish one (and vice versa) and all the related issues regarding certificate requests and ITS-S identity verification.

Author Contributions: Conceptualization, E.V., J.A., T.D. and J.F.; methodology, E.V. and J.A.; software, E.V.; validation, E.V., T.D. and A.V.S.; formal analysis, J.A. and J.F.; investigation, E.V. and J.A.; resources, J.A., T.D. and A.V.S.; data curation, E.V.; writing—original draft preparation, E.V. and J.A.; writing—review and editing, J.F., T.D., A.V.S., and L.M.; visualization, E.V. and J.A.; supervision, J.F. and L.M.; project administration, J.F. and L.M.; funding acquisition, J.F. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project STEROID with Nr. 069989 (POCI-01-0247-FEDER-069989)].

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to the complex structure of the logging mechanisms used, thus requiring an organized description of the data fields stored.

Acknowledgments: The authors would like to acknowledge the support of C-Roads Portugal project, with Grant Agreement INEA/CEF/TRAN/M2016/1363245, co-financed by the Connecting Europe Facility Program of the European Commission's Innovation and Networks Executive Agency (INEA).

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the study's design; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. C-Roads. The Platform of Harmonised C-ITS Deployment in Europe. Available online: https://www.c-roads.eu/ (accessed on 29 December 2022).
2. USDOT ITS Research. Connected Vehicle Pilot Deployment Program. Available online: https://www.its.dot.gov/pilots/ (accessed on 16 February 2023).
3. Zhi, P.; Zhao, R.; Zhou, H.; Zhou, Y.; Ling, N.; Zhou, Q. Analysis on the Development Status of Intelligent and Connected Vehicle Test Site. *Intell. Converg. Netw.* **2021**, *2*, 320–333. [CrossRef]
4. Javed, M.A.; Zeadally, S.; Hamida, E.B. Data analytics for Cooperative Intelligent Transport Systems. *Veh. Commun.* **2019**, *15*, 63–72. [CrossRef]
5. The STEROID Project. Verification and Validation of ADAS Components for Intelligent Vehicles of the Future. Available online: https://steroid-project.pt/ (accessed on 17 January 2023).
6. Du, Y.; Chowdhury, M.; Rahman, M.; Dey, K.; Apon, A.; Luckow, A.; Ngo, L.B. A Distributed Message Delivery Infrastructure for Connected Vehicle Technology Applications. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 787–801. [CrossRef]
7. Hugo, Å.; Morin, B.; Svantorp, K. Bridging MQTT and Kafka to support C-ITS: A feasibility study. In Proceedings of the 2020 21st IEEE International Conference on Mobile Data Management (MDM), Versailles, France, 30 June–3 July 2020; pp. 371–376. [CrossRef]
8. Nguyen, P.H.; Hugo, Å.; Svantorp, K.; Elnes, B.M. Towards a Simulation Framework for Edge-to-Cloud Orchestration in C-ITS. In Proceedings of the 2020 21st IEEE International Conference on Mobile Data Management (MDM), Versailles, France, 30 June–3 July 2020; pp. 354–358. [CrossRef]
9. Lu, M.; Blokpoel, R.; Fünfrocken, M.; Castells, J. Open architecture for internet-based C-ITS services. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 7–13. [CrossRef]
10. Naudts, D.; Maglogiannis, V.; Hadiwardoyo, S.; van den Akker, D.; Vanneste, S.; Mercelis, S.; Hellinckx, P.; Lannoo, B.; Marquez-Barja, J.; Moerman, I. Vehicular Communication Management Framework: A Flexible Hybrid Connectivity Platform for CCAM Services. *Future Internet* **2021**, *13*, 81. [CrossRef]
11. Gozalvez, J.; Sepulcre, M.; Bauza, R. IEEE 802.11p vehicle to infrastructure communications in urban environments. *IEEE Commun. Mag.* **2012**, *50*, 176–183. [CrossRef]
12. Laha, M.; Datta, R. A Budgeted Maximum Coverage based mmWave Enabled 5G RSUs Placement in Urban Vehicular Networks. In Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 5–9 January 2021; pp. 387–395. [CrossRef]
13. Aniss, H. Overview of an ITS Project: SCOOP@F. In Proceedings of the Communication Technologies for Vehicles, San Sebastian, Spain, 6–7 June 2016; Springer International Publishing: Cham, Switzerland, 2016; pp. 131–135.
14. Passchier, I.; Spaanderman, P.; Sambeek, M.v.; Matthews, E.; Latte, J.; Esposito, M.C.; Fouchal, H.; Lewyllie, P.; Lunnon, C.; Warren, P.; et al. Milestone 4—Common Set of Upgraded Specifications for Hybrid Communication. Version 2.1. InterCor Consortium, January 2019. Available online: https://intercor-project.eu/wp-content/uploads/sites/15/2019/03/InterCor_M4-Upgraded-Specifications-Hybrid_v2.1-final_INEA-1.pdf (accessed on 25 February 2023).
15. CONCORDA (Connected Corridor for Driving Automation). Available online: https://ertico.com/concorda/ (accessed on 17 February 2023).
16. NordicWay 3. Available online: https://www.nordicway.net/ (accessed on 29 December 2022).
17. Karkhanis, P.; Brand, M.G.v.d.; Rajkarnikar, S. Defining the C-ITS Reference Architecture. In Proceedings of the 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), Seattle, WA, USA, 30 April–4 May 2018; pp. 148–151. [CrossRef]
18. Ferreira, J.; Fonseca, J.; Gomes, D.; Barraca, J.; Fernandes, B.; Rufino, J.; Almeida, J.; Aguiar, R. PASMO: An open living lab for cooperative ITS and smart regions. In Proceedings of the 2017 International Smart Cities Conference (ISC2), Wuxi, China, 14–17 September 2017; pp. 1–6. [CrossRef]
19. Strobl, S.; Klöppel-Gersdorf, M.; Otto, T.; Grimm, J. C-ITS Pilot in Dresden – Designing a modular C-ITS architecture. In Proceedings of the 2019 6th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Cracow, Poland, 5–7 June 2019; pp. 1–8. [CrossRef]
20. Larini, G.; Romano, G.; Falcitelli, M.; Noto, S.; Pagano, P.; Djurica, M.; Karagiannis, G.; Solmaz, G. Autonomous Driving Progressed by oneM2M : The Experience of the AUTOPILOT Project. In Proceedings of the 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 June 2019; pp. 204–208. [CrossRef]
21. 5G Public Private Partnership (5G PPP). *5G Trials for Cooperative, Connected and Automated Mobility along European 5G Cross-Border Corridors-Challenges and Opportunities*. Version 1.0; European Commission, October 2020. Available online https://5g-ppp.eu/wp-content/uploads/2020/10/5G-for-CCAM-in-Cross-Border-Corridors_5G-PPP-White-Paper-Final2.pdf (accessed on 25 February 2023).
22. Ribeiro, J.; Moura, L. A-to-Be experience: Deploying a Portuguese highway C-ITS network under C-ROADS Portugal. In Proceedings of the Virtual ITS European Congress, Virtual Event, 9–10 November 2020.
23. Osório, A.L.; Moura, L.; Costa, R.; Borges, P. Towards Intelligent Mobility: The Mobility Intelligent Cooperative Systems (MOBICS) Platform. In Proceedings of 7th Transport Research Arena TRA 2018, Vienna, Austria, 16–19 April 2018.

24. u-blox. Positioning & Wireless Communication Technologies. Available online: https://www.u-blox.com/en/ (accessed on 17 January 2023).
25. IEEE. *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; Technical Report 802.11-2016; Institute of Electrical and Electronics Engineers (IEEE): Piscatway, NJ, USA, 2016.
26. ISO. *Information Security, Cybersecurity and Privacy Protection—Evaluation Criteria for IT Security—Part 2: Security Functional Components*; Technical Report 15408-2; International Organization for Standardization (ISO): Geneva, Switzerland, 2008.
27. ISO. *Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Pecific Requirements—Part 2: Logical Link Control*; Technical Report 8802-2:1998; International Organization for Standardization (ISO): Geneva, Switzerland, 1998.
28. ETSI. *Intelligent Transport Systems (ITS);Vehicular Communications; GeoNetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-Part 1: Media-Independent Functionality*; Technical Report EN 302 636-4-1 V1.4.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
29. Deering, S.; Hinden, B. RFC 2460: Internet Protocol, Version 6 (IPv6) Specification, 1998. Available online: https://www.rfc-editor.org/rfc/rfc2460 (accessed on 29 December 2022).
30. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-Part 1: Transmission of IPv6 Packets over GeoNetworking Protocols*; Technical Report EN 302 636-6-1 V1.2.0; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2013.
31. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-Part 1: Basic Transport Protocol*; Technical Report TS 302 636-5-1 V2.1.0; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2017.
32. Postel, J. RFC 768: User Datagram Protocol, 1980. Available online: https://www.rfc-editor.org/rfc/rfc768 (accessed on 29 December 2022).
33. Postel, J. RFC 793: Transmission Control Protocol, 1981. Available online: https://www.rfc-editor.org/rfc/rfc793 (accessed on 29 December 2022).
34. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*; Technical Report EN 302 637-2 V1.4.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
35. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*; Technical Report EN 302 637-3 V1.3.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
36. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities Layer Protocols and Communication Requirements for Infrastructure Services*; Technical Report TS 103 301 V1.2.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2018.
37. ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2*; Technical Report TR 103 562 V2.1.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
38. ETSI. *Intelligent Transport Systems (ITS); Facilities Layer Function; Part 1: Services Announcement (SA) Specification*; Technical Report EN 302 890-1 V1.2.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
39. ETSI. *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*; Technical Report TS 103 097 V1.3.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2017.
40. ETSI. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*; Technical Report TS 102 941 V1.3.1; European Telecommunications Standards Institute (ETSI): Sophia Antipolis, France, 2019.
41. IEEE. *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages—Amendment 1*; Technical Report 1609.2a-2017; Institute of Electrical and Electronics Engineers (IEEE): Piscatway, NJ, USA, 2017.
42. Correia, M.; Almeida, J.; Bartolomeu, P.C.; Fonseca, J.A.; Ferreira, J. Performance Assessment of Collective Perception Service Supported by the Roadside Infrastructure. *Electronics* **2022**, *11*, 347. [CrossRef]
43. Rocha, D.; Teixeira, G.; Vieira, E.; Almeida, J.; Ferreira, J. A Modular In-Vehicle C-ITS Architecture for Sensor Data Collection, Vehicular Communications and Cloud Connectivity. *Sensors* **2023**, *23*, 1724. [CrossRef] [PubMed]
44. Almeida, T.T.; de C. Gomes, L.; Ortiz, F.M.; Júnior, J.R.; Costa, L.H.M.K. IEEE 802.11p Performance Evaluation: Simulations vs. Real Experiments. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 3840–3845. [CrossRef]