Multi-Radio V2X Communications Interoperability Through a Multi-access Edge Computing (MEC)

Jordi Casademont[1,2*], Bruno Cordero[1], Daniel Camps-Mur[1], Luís Alexandre Morais da Conceição[3], Aris Lalos[4,5], Christian Vitale[6], Christos Laoudias[6], Pouria Sayyad Khodashenas[1]

[1] *i2CAT Foundation, Barcelona, Spain*
[2*] *Universitat Politècnica de Catalunya, Barcelona, Spain. E-mail: jordi.casademont@upc.edu*
[3] *Ubiwhere, Aveiro, Portugal*
[4] *University of Patras, Rio, Patras, Greece*
[5] *Industrial Systems Institute, ATHENA Research Centre, Patras, Greece*
[6] *KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus*

ABSTRACT
Nowadays, we are ready to have precommercial Cooperative Intelligent Transport Systems (C-ITS), nevertheless there exist challenging functional and security aspects that need to be addressed. One of them is the fact that, in every era, there will be several radio technologies which will be used by vehicles that need to be connected between them, therefore, the systems needs to provide interoperability services. The other critical issue is to reinforce security against attacks on localization receivers or in vehicles equipment. Most of these functions are based in a large amount of computation power, to this end, this paper presents the approach taken by H2020 CARAMEL project, using a Multi-access Edge Computing (MEC) that could provide the necessary performance assets.
Keywords: C-ITS, V2X, DSCR, C-V2X, MEC, GPS spoofing

1. INTRODUCTION

The ecosystem of vehicles connected to everything (V2X) and Cooperative Intelligent Transport Systems (C-ITS) has been working in developing standards, building prototypes and deploying real testbeds for more than ten years. Now, it is time to start the industrialization phase and to deliver final products to the consumers. Nevertheless, this phase introduces new implementation challenges and the need to implement different linked subsystems.

Firstly, we have to deploy the communications system between vehicles (V2V: Vehicle-to-Vehicle) and between vehicles and the support infrastructure (V2I: Vehicle-to-Infrastructure). The main concern is that, nowadays, there are different stakeholders supporting different radio technologies, so, initial scenarios will have to deal with multi-radio situations and make the necessary steps to enable interoperation between vehicles using different radio communication systems.

Secondly, it is necessary to set up a Public Key Infrastructure (PKI) system to provide the necessary elements for ensuring security in the V2X communications between the involved entities. Currently, the European Telecommunications Standards Institute (ETSI) has one standard [1] that foresees most of these functions, but some critical points, as the Certificate Revocation List (CRL) distribution, is not yet addressed.

Finally, there is the On-Board Unit (OBU) which is the communications hardware to be deployed in vehicles and it has to address security measures to make the whole system trustful for users. One of the possible attack vectors to V2X infrastructure is to steal sensitive data or cryptographic keys from the vehicle's OBUs. In order to counter this attack, trustworthy, unforgeable, and non-copiable identities must be established for the V2X communication partners. One way to achieve this goal is to integrate a Hardware Security Module (HSM) into the OBU that serves as a repository for private key data as well as a cryptographic processor for sensitive operations. Additionally, most of C-ITS services are based on vehicle's position, mostly obtained using Global Navigation Satellite System / Real-Time Kinematics (GNSS/RTK) receivers which can be attacked using location spoofing. Therefore, the global system has to perform some action to detect when vehicles are location spoofed and act consequently.

Clearly, a fully operational C-ITS system demands a big deal of support mechanisms that require high computation power, more than the one provided by Road Side Units (RSU) or OBUs. In the ongoing H2020 CARAMEL project, we propose to use a Multi-access Edge Computing (MEC) that could provide the necessary performance assets.

This paper is structured as follows. Section 2 introduces the open problems that could be solved by the usage of a MEC in the fixed infrastructure of a C-ITS system. Section 3 describes the possible architecture of such a MEC. Section 4 presents the approach of MEC interaction with the other subsystems taken by CARAMEL. Finally, section 5 summarizes and concludes the paper.

2. Open problems for a secure C-ITS architecture

In order to deploy a fully functional secure C-ITS system we face two main groups of technical challenges: the co-existence of different radio technologies and the mechanisms to reinforce security in communications and position measurements.

2.1 V2X Radio Technologies and interoperability

V2X communications require new protocol architectures that differ from the standard TCP/IP model used in Internet. Nowadays, there are two main architectures, the European based on the GeoNetworking (GN) protocol and Basic Transport Protocol (BTP), standardized by the ETSI, and the North-American based on the WAVE (Wireless Access in Vehicular Environments) architecture, standardized by the Institute of Electrical and Electronics Engineers (IEEE). Although they differ in the upper layer protocols (from network layer and up) there is no much problem because each one will be used in specific regions and it is not foreseen to have areas with vehicles using both architectures.

The main controversy is in the Physical and Link layers which contain the radio technologies to be used around the world, independently on which upper layer protocols are. Nowadays, there are two main lines of technologies, both with one working standard and a new version in development. The more mature is IEEE 802.11p, standard published in 2010 also known as Direct Short-Range Communications (DSCR). Later it came the proposal from 3rd Generation Partnership Project (3GPP), an enhancement of the Long Term Evolution (LTE) published in Release 14, in 2017, also known as Cellular V2X (C-V2X) or LTE-V2X. Moreover, LTE-V2X employs different radio interfaces: i) interface between the vehicle and eNB, named LTE-Uu, and ii) interface between vehicles, named PC5. While these two technologies are commercially fighting to get chosen by the vehicle industry, they are working on the new standards IEEE 802.11bd and 5G NR-V2X.

The fact is that, as for early 2020, some vehicles manufacturers, as Volkswagen, have began to distribute vehicles with IEEE 802.11p and shortly, there will be other cars equipped with LTE-V2X. This raises the problem that vehicles using different radio technologies will not be able to communicate directly between them. Apart from having vehicles equipped with multiple technologies, the solution is to relay on functions performed by the fixed network and have communications V2I2V (Vehicle-to-Infrastructure-to-Vehicle). Nevertheless, due to the strict end-to-end delay restrictions required by some C-ITS applications, it seems that the use of a MEC could provide the necessary performance values.

Moreover, a part from the intrinsic communications between vehicles that a C-ITS system must have, it is also necessary another parallel protocol architecture, based on TCP/IP, to have semi-permanent connection with the PKI servers to manage cryptographic material (Authorization Tickets, certificate revocation) and alarms when the car is being attacked: HSM tampering, GPS spoofing and new attacks that the car may detect in the future. This channel can also be used to download software updates.

2.2 Attack discovery and decision-making process

Once the system is deployed, an on-going process to detect attacks must be initiated. Among the different architecture's elements that may be attacked, two of them are the most critical. Firstly, one attack vector would be to try to stole the cryptographic keys in one vehicle's OBU. So that, the HSM in which the keys are stored, when is under attack it must perform two basic operations, delete any information of its memory, and notify to the management infrastructure that it has suffered a tampering attack. The second critical vector attack is when the vehicle is under GPS spoofing and it broadcasts a false location information. In this case, there are two techniques to counter this attack, one is performed in the same OBU and another is performed in the main fixed infrastructure. In both cases, when this attack is detected, the management infrastructure must be informed that one or several cars are transmitting false information.

Whenever one of these two attacks have been informed about, one process must decide if the cars under attack should be disallowed transmitting signed messages. In case they are revoked, the PKI servers must be notified and certificates to sign messages should be revoked. Next step is to distribute this information among the cars in the vicinity of the, now, unauthorized vehicles. The distribution of Certificate Revocation Lists (CRL) is not a trivial issue due to its scalability problem [2], but its criticality for safety applications forces to have a process to address this distribution, at least, to the most critical areas.

3. System architecture with MEC

The fixed infrastructure of a C-ITS system is formed by four different subsystems (figure 1): base stations for the radio technologies (IEEE802.11p RSUs and LTE-Uu Small Cells), the fixed communication system (Ethernet over optical fibre or wireless links), the PKI and the MEC. Vehicles can be provided with one or two radio interfaces. While LTE-Uu is compulsory to be able to authenticate vehicles, 802.11p is optional.

The PKI architecture comprises five different servers, four of them are standardized by ETSI in [1] and the fifth is a new proposal to manage certificate revocation. Those present in [1] are two certification authorities, the main Root Certification Authority (RCA) which is offline and contains root certificates for the entire PKI and the other is the Online Certification Authority (OCA) to sign the different lower authorities in the PKI, then we have the Enrolment Authority (EA) and the Authorization Authority (AA) which roles are authenticate and authorize vehicles respectively. The Validation Authority (VA) is an extension proposal to provide Certificate Revocation Lists along with an online service that returns the state of specific certificates in real-time.

The MEC server will be deployed to accommodate the required functions to run at the edge of the network, following, as much as possible, the ETSI MEC framework standardization [3] (Figure 2). To pursue the requirements of CARAMEL, it is intended to provide a framework that enables the deployment and management of MEC applications in a dynamic and flexible way, comprising of the following sub-components:

- Dashboard module: Provides a user interface to deploy and manage MEC apps, closing the gap between the user and the orchestrator.
- Orchestrator: Manages MEC servers and their applications.
- MEC Server: Contains compute and network resources, on top of which the MEC host will run and provide a virtualized infrastructure to run applications.

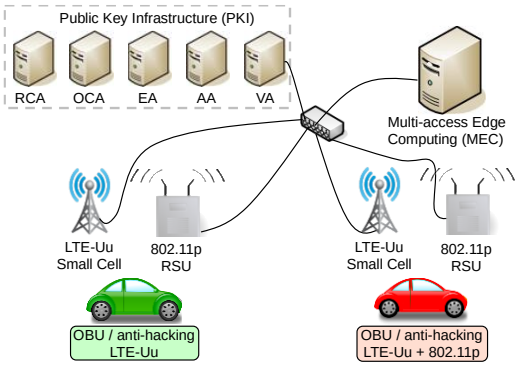

Figure 1. General architecture of the secure ITS system.

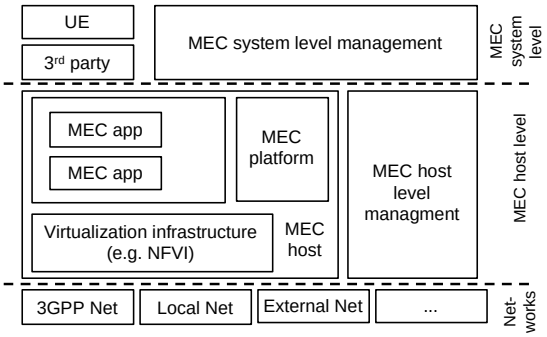

Figure 2. MEC architecture.

The MEC runs two types of applications. The first group includes applications that perform user level functionalities and are introduced in the next section. The second group of applications comprise those that send and receive messages generated by applications of the first group to and from the radio interfaces in the RSUs and Small Cells. It is necessary to implement two different protocol architectures, the traditional TCP/IP to interchange security messages about vehicle's authentication, authorization and certificates, and the ETSI ITS G5 with GeoNetworking and BTP protocols. While the TCP/IP is directly implemented by the main operating system of the MEC server, the ITS G5 needs additional software. In our case, we have chosen the opensource Vanetza framework [4] that is able to handle basic CAM and DENM messages and encapsulate them over BTP/GN. The main problem is that all these messages are sent digitally signed, and the process to generate and check digital signatures is CPU consuming, for this reason this process is executed in the MEC and not in the radio equipment (RSU/Small Cells). Therefore, the MEC will run a virtualized instance of this protocol stack for each radio equipment, as if decoupling each RSU/Small Cell in two parts, the most computation demanding part in the MEC and the basic radio functions in the radio equipment. This proposal has an extra concern, which is that both protocol architectures expect to have the radio interface directly attached to the equipment in which run. The proposed solution is to virtualize one ethernet interface in every virtual container that runs one protocol architecture for each radio equipment, and using a VLAN capable switch, we can transparently relay these frames to each radio equipment, which will directly forward any message received from its VLAN Ethernet interface to the radio interface. Finally, most of ITS G5 messages are sent to the broadcast address, as their information is intended to be received by all vehicles in the vicinity of the transmitter. The problem is that, while IEEE802.11p equipment is broadcast capable, most LTE-Uu Small Cells are not. Although LTE standard defines the evolved Multimedia Broadcast Multicast Services (eMBMS) it is not widely deployed. Therefore, to cope with this inconvenient if necessary, the MEC has to run an additional application that registers all vehicles in the system, under which Small Cell are they operating, and transform a broadcast transmission over LTE-Uu in multiple unicast transmissions to every vehicle that needs to receive the message.

4. Security and interoperability services running in the MEC platform

C-ITS systems require management and control applications which need a large amount of computation power. In CARAMEL project we propose an initial set of three applications for security and multi-radio interoperability.

4.1 Process: C-ITS Messages management for multi-radio interoperability

The radio infrastructure deployed in the operative region of the C-ITS system will receive and forward all ITS messages transmitted by vehicles to the interoperation application running in the MEC. This application is in charge of validating these messages by checking their digital signature, analyse their GeoNetworking header to know the geographical area for which these messages are intended to be distributed and, finally, to retransmit them through the required radio technologies, 802.11p or/and LTE-Uu.

4.2 Process: GPS spoofing attack detection

In a GPS spoofing attack, the GNSS/RTK receiver is attacked by injecting via broadcasting, incorrect GPS signals, structured to resemble a set of normal GPS signals. These spoofed signals mislead the estimation process that takes place in the receiver, predicting a position that is different from the actual one. Two different approaches are considered and deployed for identifying this type of attack, one is executed locally in the vehicle, the other takes place in the MEC, by deploying a self-localization integrity check and then a collaborative position estimation.

The self-localization leverages in-vehicle measurements for attack detection. This solution employs absolute vehicle location information (e.g., derived through cellular network localization techniques) and fuses them with vehicle on-board sensory data (e.g., accelerometer, steering angle, etc.) by means of Bayesian filtering (e.g., Kalman filter) to compute a vehicle's estimated location stream. This stream is compared to the vehicle's GPS data stream using a location integrity check scheme that is able to detect GPS location spoofing attacks. In this sense, this approach is complementary to the collaborative approach and they can be combined to increase the overall attack detection accuracy and reliability.

In the collaborative approach for GPS integrity check, we consider a vehicular network of N interconnected vehicles that are deployed on the road and are moving constantly. Each vehicle transmits at each time instant to the MEC platform (i) its absolute position measurement from GPS, (ii) the relative distance measurement between neighbouring vehicles and (iii) the relative azimuth angle or angle of arrival measurement between neighbouring vehicles using LIDAR/RADAR sensor. The accuracy of the estimation process, which is robust to potential attacks, is performed by fussing the 3 measurement models. This is achieved by defining and solving a multi modal optimization function that treats vehicles as nodes in a planar graph with arbitrary connectivity and a sparse set of control points (those that have passed the local integrity check), allowing the reconstruction of the geometry of the rest points in the graph, that correspond to the estimated position for all the vehicles, by solving a sparse linear system.

4.3 Process: Certificate revocation and list distribution

PKI servers are designed to manage vehicles' authentication and authorization and to distribute certificates to sign messages. Nevertheless, in some situations, vehicles should be deauthorized due to several possible reasons. In these cases, a process running in the MEC should provide the necessary intelligence to decide if the vehicle needs to be deauthorized or not and, spread this information to the vehicles driving in the area of interest of this information by distribution of Certificate Revocation Lists (CRL). This distribution process implies an important scalability problem, so our proposal is to use a Publish/Subscribe model to selectively distribute the CRLs to vehicles that really may use this information before the natural expiration of the certificates due to their age.

5. CONCLUSIONS

In this paper we have presented the functional and security functions that need to be performed in an operative C-ITS system. We have put forward the necessity of multi-radio interoperability between the current available radio technologies (IEEE802.11p and LTE-Uu) and the requirement to reinforce the basic security system through functions that detect vehicles misbehaviours due to external attacks as GPS spoofing or physical attacks as tampering attempts to access to the vehicle's cryptographic material. In both cases, it should be advisable to deploy a system to distribute CRL. As most of these functions require a high level of computation, we present the proposal of project H2020 CARAMEL, which it is to use a MEC that controls and supports several radio base stations.

ACKNOWLEDGEMENTS

This work was supported by the European Union's H2020 research and innovation programme under CARAMEL project (Grant agreement No. 833611). The work of J. Casademont and P. Sayyad Khodashenas was also supported by FEDER and Secretaria d'Universitats i Recerca del Departament d'Empresa i Coneixement de la Generalitat de Catalunya through project Fem IoT. The work of C. Vitale and C. Laoudias was also supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 739551 (KIOS CoE) and from the Republic of Cyprus through the Directorate General for European Programmes, Coordination and Development.

REFERENCES

[1] ETSI: TS 102 940 V1.3.1 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. April 2018.

[2] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas, A. Nix: Optimized Certificate Revocation List Distribution for Secure V2X Communications, Vehicular Technology Conference (VTC-Fall), Canada, 2017.

[3] ETSI: GS MEC 003 V2.1.1. Multi-access Edge Computing (MEC); Framework and reference architecture. January 2019.

[4] R. Riebl: Vanetza framework, Open-source implementation of the ETSI C-ITS protocol stack. Technische Hochschule Ingolstadt. https://github.com/riebl/vanetza [Accessed April 2020].