The CARAMEL Project: a Secure Architecture for Connected and Autonomous Vehicles

Christian Vitale*, Nikos Piperigkos†**, Christos Laoudias*, Georgios Ellinas*, Jordi Casademont‡‡, Pouria Sayyad Khodashenas§, Andreas Kloukiniotis**, Aris S. Lalos†**, Konstantinos Moustakas**, Pablo Barrientos Lobato††, Javier Moreno Castillo†‡, Petros Kapsalas§ and Klaus-Peter Hofmann xi

* KIOS Research and Innovation Center of Excellence, University of Cyprus, Nicosia, Cyprus
† Industrial Systems Institute, Athena Research and Innovation Center, Patras, Greece
** Dept. of Electrical and Computer Engineering, University of Patras, Patras, Greece
†† i2CAT Foundation, Barcelona, Spain
§ Universitat Politècnica de Catalunya, Barcelona, Spain
‡‡ Atos IT Solutions and Services Iberia S.L., Madrid, Spain
†† FICOSA, Barcelona, Spain
‡ Panasonic Automotive, Langen, Germany
xi T-Systems International GmbH, Frankfurt, Germany

Abstract—The main goals of the CARAMEL project are to enhance the protection of modern vehicles against cybersecurity threats related to automated driving, smart charging of Electric Vehicles, and communication among vehicles or between vehicles and the roadside infrastructure. This work focuses on the latter and presents the CARAMEL architecture for improving the security and privacy of communication for connected and autonomous driving. The proposed architecture includes: (i) multi-radio access technology capabilities, with simultaneous 802.11p and LTE-Uu support; (ii) a MEC platform, where algorithms for detecting attacks are implemented; (iii) an intelligent On-Board Unit with anti-hacking features inside the vehicle; (iv) a Public Key Infrastructure that validates in real-time the integrity of vehicle’s data transmissions. As an indicative application scenario, the interaction between the entities of the CARAMEL architecture is showcased in the case that the GPS locations used by vehicles are spoofed.

I. INTRODUCTION

The damaging effects of cyberattacks to an industry like the Cooperative Connected and Automated Mobility (CCAM) can be tremendous. From the least to the most important one, it is possible to mention the damage in the reputation of vehicle manufacturers, the increased denial of customers to adopt CCAM, the loss of working hours (having direct impact on the European GDP), increased environmental pollution due to, e.g., traffic jams or malicious modifications in sensors’ firmware, and, finally, the great danger for human lives, either they are drivers, passengers or pedestrians. The goal of the CARAMEL project is to proactively address modern vehicle cybersecurity challenges applying, among others, advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, and to seek methods to mitigate associated safety risks.

To address cybersecurity considerations for the already here Connected and Autonomous Vehicles (CAVs), well established methodologies coming from the ICT sector will be adopted, allowing to assess vulnerabilities and the impacts of potential cyberattacks. Although past initiatives and cybersecurity projects related to the automotive industry have improved security for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily yet. Considering the entire supply chain of automotive operations, CARAMEL targets to reach to commercial anti-hacking Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios. Specifically, CARAMEL focuses on three main types of attacks: (i) attacks on the AI of autonomous vehicles: computer vision and AI techniques are crucial for vehicle self-driving and environment understanding; (ii) attacks on the electric vehicle charging infrastructure: the rise in adoption of EVs is gaining momentum and the misuse of the charging infrastructure could have effects on the national and Europe’s energy sustainability; (iii) attacks on the communication infrastructure underlying CCAM, which could impair the overall system performance.

In this paper we focus on one of the three pillars of CARAMEL, i.e., defending against attacks on the CCAM connectivity infrastructure. In Section II, we present the secure connectivity architecture envisioned in CARAMEL. Then, in Section III, we overview the attacks that a connectivity infrastructure may face, with the corresponding state-of-the-art solutions. The three attacks taken into consideration for demonstration in CARAMEL are also outlined. Finally, in Section IV the interactions among different entities in the proposed architecture are exemplified in a GPS location spoofing attack scenario and an effective countermeasure is described.

II. THE CARAMEL ARCHITECTURE

The CARAMEL’s objective is to propose a secure environment for autonomous and connected vehicles. As part of this objective, the security and the privacy aspects of the adopted
communication infrastructure play a crucial role. CARAMEL will advance existing state-of-the-art solutions by combining a Multi-Radio Access Technology (Multi-RAT) V2X communication infrastructure with ML algorithms running both at the vehicle, in the so-called On-Board Unit (OBU), and at the network edge, i.e., at the Multi-access Edge Computing (MEC) platform. Thanks to the implemented ML algorithms, CARAMEL keeps track of the integrity and of the validity of the information transmitted in the system and it exploits a Private Key Infrastructure (PKI) to register and authorize all vehicles’ data transmissions, e.g., by updating or canceling distributed certificates when problems are detected. Figure 1 summarizes the CARAMEL secure multi-technology V2X telecommunications infrastructure.

![Image](74x420 to 275x559)

Fig. 1: Secure Multi-Technology V2X Telecommunications Infrastructure.

A. The Public Key Infrastructure (PKI)

This element basically comprises five different servers:

- The Root Certification Authority (RCA): This server must be managed only by authorized personnel and contains the root certificates for the entire PKI;
- The Online Certification Authority (OCA): This is an online server signed by the RCA. Its main responsibility is to sign the different lower authorities in the PKI;
- Enrolment Authority (EA): This entity is in charge of providing the necessary certificates at the enrolment phase, which are used by the car to ask for pseudonym certificates or Authorization Tickets (AT);
- Authorization Authority (AA): This entity manages the pseudonym certificates, which are issued for ensuring privacy of the cars within the PKI;
- Validation Authority (VA): This entity provides a way to ask the PKI which certificates are revoked. It provides a Certificate Revocation List (CRL) with the revoked certificates, along with an online service that returns the state of a specific certificate in real-time.

In the enrolment phase, an Intelligent Transport System (ITS), e.g., an Autonomous Vehicle (AV), requests enrolment credentials to an EA such that it can be trusted to function correctly by other ITS stations. In the authorization phase, an enrolled ITS station requests pseudonymous ATs to an AA to get specific permissions, ensuring confidentiality and privacy. Internally, the AA asks the VA to check if the request is authorized. Finally, EA and AA can be trusted by ITS stations through validating their authenticity with the RCA. The PKI enables the provision of secure V2X message transmissions and will be the basis to the certificate management of vehicles.

B. The Multi-RAT V2X communication infrastructure with MEC functionalities

As of the beginning of 2020, there is not a clear radio technology to be used for V2X communications. Up to now, IEEE 802.11p has been the de facto wireless technology standard for V2X communications. It is a relatively mature technology and has already been validated by over a decade of field trials. Despite that, IEEE 802.11p, which uses Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA), suffers from a high level of collisions under heavy traffic conditions, mainly due to hidden terminal situations. Long-Term Evolution (LTE)-based V2X from the Third Generation Partnership Project (3GPP) is a relatively new alternative solution to the IEEE 802.11p-based V2X communications. The first version of LTE-V2X came with numerous enhancements to the existing Device-to-Device (D2D) communications to accommodate vehicular communications. These enhancements include a new arrangement of the resource grid of the physical layer and two types of D2D channel access mechanisms: (i) a mechanism coordinated by the evolved NodeB (eNB), named Mode 3, and (ii) a distributed mechanism, where User Equipments (UE) access the channel on their own, named Mode 4. Moreover, LTE-V2X employs different radio interfaces: (i) interface between the vehicle and eNB, named LTE-Uu, and (ii) interface between vehicles, named LTE-PC5.

The objective of CARAMEL is to address the securitisation of V2X communications using the certificates distributed by the PKI architecture, and the interoperability between IEEE 802.11p, which works in the Control Channel (CCH) of the ITS-G5 band (5.9 GHz), and C-V2X technologies, which is implemented with interface LTE-Uu radio working in the operator’s band. Interoperability between both technologies is implemented using infrastructure support through the use of MEC. The MEC infrastructure is hosted on a server which offers both the virtualized environment for MEC applications to be instantiated on, e.g., for vehicle safety, as well as the required V2X physical interfaces to the different underlying radio access technologies. Moreover, it will have rules to decide which messages to forward and where to forward them. These rules enable the forwarding, filtering and dropping of messages according to their importance, age, region of interest, etc. It is possible to simply replicate messages transmitted with one technology to the other one, or forward messages to other regions covered with other base stations.

C. The vehicle’s On-Board Unit

Standard cooperative cars are equipped with an OBU which provides secure communication functionalities. The objective of CARAMEL is to develop a completely functional OBU that complies with current security regulations and to combine
it with a so-called “Anti-Hacking Device” that is able to detect hacking attempts and functional misbehaviours using ML-based algorithms and techniques. The OBU architecture, shown in Figure 2, includes the following main elements:

1) Hardware Security Module (HSM): One of the possible attack vectors to V2X infrastructure is to steal sensitive data or cryptographic keys from a vehicle’s OBU. To counter this attack, trustworthy, unforgeable and non-copyable identities must be established. This is achieved by integrating an HSM into the OBU that serves as a repository for private key data (for authentication and encryption purposes), as well as a cryptographic processor for sensitive operations. The HSM is the main component to prevent and counter attacks as the tampering of the OBU (Section III-B2).

2) Radio interfaces (IEEE 802.11p and LTE-Uu): Radio interfaces are crucial in CARAMEL for connecting to the PKI servers to obtain the pseudonymous ATs before being able to transmit ITS messages and for real-time management of certificates. For this purpose, LTE-Uu will be used. For data transmission, direct V2V connections are preferred, instead of V2I, to reduce latency during ITS message transmission. Regarding V2V connections, IEEE 802.11p is used in CARAMEL due to its maturity. Lastly, we consider two types of cars, i.e., those that feature both radio interfaces (LTE-Uu and 802.11p) and are able to perform V2V connections, and those that are only able to connect to the fixed network through a single radio interface (LTE-Uu).

3) V2X Communication Protocol Architecture: This element contains the software package that enables the OBU to generate Facilities layer messages encapsulated on the Basic Transport Protocol (BTP) and the GeoNetworking protocol (GN). CARAMEL will use the open source framework Vanetza [1], that will be properly extended to perform all security and privacy related functionalities.

4) Security applications: This element contains all software functions to interact with the PKI and manage the registration and authorization procedures, as well as to obtain the pseudonymous ATs and store them into the HSM according to [2].

5) ITS Applications: This element represents any ITS application running on the vehicle. The CARAMEL testbed foresees applications for sending and receiving Cooperative Awareness Messages (CAM) and Decentralized Event Notification Messages (DENM) messages.

6) Anti-hacking Device: It extends the security capabilities of the OBU by means of advanced techniques for detecting misbehaviours and attacks; see Section IV.

III. OVERVIEW ON CARAMEL CONNECTIVITY ATTACKS

In this section, we present the potential threats and vulnerabilities that may be encountered by the CARAMEL connectivity infrastructure. We first present a general overview on the possible attacks (with available countermeasures) that can be carried out. Then, we present in detail the subset of attacks considered in CARAMEL.

A. Attacks on the CARAMEL Connectivity Infrastructure

Based on [3], the attacks can be classified into four general categories: (1) Authenticity/Identification attacks; (2) Availability attacks; (3) Confidentiality/Privacy attacks; and (4) Data integrity/Data trust attacks. Below we describe these categories and briefly discuss possible mitigation techniques.

1) Authenticity/Identification attacks: Authenticity is a prime requirement in AV networking to ensure the protection of the legitimate in-network entities against several attacks.

- Sybil attack: A malicious vehicle pretends to be legitimate by exploiting fake identities. Authenticated nodes consider the malicious messages to be legitimate and cannot detect the attackers. Cryptography schemes can be adopted as a countermeasure [4].
- Location Service Jamming and Spoofing: Global Navigation Satellite Systems, e.g., the GPS, are vulnerable to attacks where legitimate satellite signals are either blocked or counterfeited. An effective solution for detecting the location spoofing attack is presented in Section IV.

2) Availability attacks: Availability is crucial to ensure the safety of the involved drivers and vehicles.

- Denial of Service (DoS) attack: Aims to prevent legitimate entities from accessing the network services and resources. Access control with packet filtering is the recommended mitigation technique [5].
- Timing attack: A transmission is delayed by adding extra timeslots between received messages. Authenticated timing methods are effective against these attacks [6].
- Flooding and Jamming attack: Focuses on disrupting the network communication channels. Channel switching is the adopted solution [7].

3) Confidentiality/Privacy attacks: Contrary to the previous attacks, confidentiality and privacy attacks may not affect safety. Nevertheless, sensitive information exchanged in the network, e.g., locations of the AVs, ITS safety messages, and drivers’ personal information should be protected.

- Eavesdropping attack: Attempts to steal information (e.g., location) by snooping on the communication channel. Although it is easy to carry out, secure communication can be used to prevent this attack [8].
- Interception attack: Starts by listening to the network for some time and then trying to analyze the data to extract useful information. Privacy-preserving methods can be adopted to mitigate this attack [9].
4) Data integrity/Data trust attacks: Data must be intact and unchanged throughout its lifecycle. The attackers could easily alter the data or falsify data exchanged among vehicles and/or the infrastructure.

- Replay attack: Previously generated data are maliciously repeated, whereas duplicated data can be prevented by making use of the sequence number, time-stamp and secure communication [10];
- Data alteration data injection attack: Intentionally modified data are injected to the network of vehicles. Signature of transmitted packets can be used [11].

B. Attack Scenarios in CARAMEL

1) Scenario 1 – Attack on the V2X message transmission: This scenario has two main objectives. Firstly, to demonstrate the correct coordination between the PKI and vehicles to distribute the pseudonymous ATs, its use to sign V2X messages, and their verification to detect non-authorized messages or messages signed with revoked certificates. Secondly, to provide a mechanism to improve privacy. Currently, privacy is performed using pseudonymous identifiers, instead of real identifiers inside the AT and changing the AT at given intervals. However, knowing the position of the vehicles and the interval used in AT renewal, tracking by an attacker becomes trivial. In CARAMEL, an ML-based algorithm will be developed to optimize the moments when ATs are renewed. A vehicle will consider the V2X messages sent by the surrounding mobile entities, and it will decide a moment that can mislead the trackers by trying to confuse itself with the other vehicles. This algorithm will be a neural network generated by adversarial training, competing with another ML algorithm that will try to track the vehicles from the information contained in the V2X messages.

2) Scenario 2 – Tamper attack to a vehicle’s OBU: It is directed to a specific vehicle affecting privacy, and potentially, safety. The step-by-step implementation of this attack together with the countermeasure proposed in CARAMEL are as follows: (i) the attacker gets hands-on with tools to open the enclosure of the OBU and the OBU is disconnected; and (ii) the OBU detects the tampering and initiates anti-tampering mechanisms, i.e., the OBU triggers secure-state actions to protect confidential information, e.g., zeroisation of the private keys and any other confidential data.

3) Scenario 3 – GPS spoofing attack: The GPS receiver in the AV is deceived by broadcasting fake satellite signals, structured to resemble a set of normal GPS signals. These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere other than where it actually is. Typically, such an attack begins by broadcasting signals synchronized with the genuine signals observed by the target receiver. The power of the counterfeit signals is then gradually increased and drawn away from the genuine signals. Following this approach the attack is carried out in the target area using a static transmitter based on Software Defined Radio (SDR) hardware/software. CARAMEL is able to detect the location spoofing attack thanks to a parallel stream of vehicle locations that relies on GPS-free signals, e.g., in-vehicle sensor measurements. This secondary location stream is compared with the GPS locations and in case their difference exceeds a predefined threshold, an alarm is raised to signify a GPS spoofing attack.

IV. THE CARAMEL SYSTEM IN ACTION: THE GPS SPOOFING ATTACK

In this section, we describe some preliminary results on one of the three attack scenarios considered in the project, i.e., the GPS spoofing attack. We first present the framework of the attack identification with two possible implementations of the GPS location integrity check, namely one based on an in-vehicle scheme (Section IV-A1) and another one based on a collaborative approach (Section IV-A2). Then, once the attack is identified, we present the mitigation technique used in CARAMEL as a countermeasure.

A. Attack Identification

Solutions for location spoofing resilience are under study. For instance, Galileo is the first satellite system to introduce an anti-spoofing service on a civil GNSS signal through the OS-NMA (Open Service Navigation Message Authentication), i.e., a service on the Galileo E1 frequency that enables authentication of the navigation data. However, despite anticipation, no integrated circuit designs for OS-NMA on E1 have been released to date and some experts question the use of OS-NMA if receivers can deliver anti-spoofing protection based on inertial sensors or signal processing [12]. To this end, we present two alternative low-cost and fast-to-deploy solutions.

1) In-vehicle GPS location integrity check: In this approach, the CARAMEL system computes the secondary location stream for the GPS integrity check using a Bayesian filtering technique, which consists of two basic steps: (i) the prediction step; and (ii) the update step. With Bayesian filtering, the motion of the vehicle is described through the characterization of the underlying physical laws and the prediction of the future vehicle location is obtained through on-board sensors. Subsequently, GPS-free global location measurements obtained by an alternative location system inside the vehicle are employed to update the previously predicted location. Potentially, depending on the quality of the global location measurements used in the update step, the CARAMEL system could revert to the secondary location stream to steer temporarily the vehicle, while the attack is in place. Figure 3 summarizes the steps of the proposed approach. Notably, the solution adopted in CARAMEL is modular, and each block could be modified based on the available on-board sensors and on the available GPS-free global location measurements.

For demonstration, the following prediction and update steps are considered in CARAMEL. The secondary location stream is implemented as a container within the anti-hacking device of the vehicles’ OBU, as shown previously in Figure 2. The software has access to the CAN bus data, specifically to the steering angle ($\alpha$), the yaw rate ($\dot{\phi}$), and the wheel speed ($v$) sensor data. By employing the Inertial Measurement Unit
Fig. 3: In-vehicle GPS location integrity check.

(IMU) readings that are readily available, it is possible to build a non-linear bicycle model of the vehicle state following the underlying physical laws. A bicycle model is built under the basic assumption that the motion of a vehicle can be well approximated by a bicycle, i.e., collapsing the rear and the front axes into a single point. Given the adopted bicycle model, we describe the motion of the vehicle considering the involved inertial forces, e.g., the friction of the wheels on the pavement. We first describe the prediction step for the vehicle movement relatively to its body-frame, i.e., having the x-axis direction as the heading of the vehicle:

\[
\begin{align*}
\dot{x}_{k+1}^f &= v \Delta t \\
\dot{x}_{k+1}^r &= v \\
y_{k+1}^f &= (C_f (\alpha - \frac{L_f \phi}{v}) + C_r (\frac{L_r \phi}{v}) ) \Delta z^2, \\
y_{k+1}^r &= (C_f (\alpha - \frac{L_f \phi}{v}) + C_r (\frac{L_r \phi}{v}) ) \Delta z^2 \\
\end{align*}
\]

where \( L_f \) and \( L_r \) are the distance of the front wheel and the rear wheel from the mass barycentre, respectively, \( M \) is the mass of the vehicle, \( C_f \) and \( C_r \) represent the corner stiffness of the front and rear wheels, respectively. Given the one-step prediction of the vehicle movement in its body-frame, a simple coordinate transformation is applied to obtain an one-step prediction in the global geographic reference system. The associated covariance of the estimated position is computed with a Bayesian Filter e.g., an Extended Kalman Filter (EKF) approach. The EKF is also used to fuse the obtained predicted vehicle location with a GPS-free location measurement. In the update step of the EKF, we assume to obtain a global location measurement of the vehicle through signals of opportunity (SOOP) [13]. In SOOP, a passive receiver located at the vehicle scans a predetermined set of frequencies where transmitters are typically active, e.g., LTE and Road Side Units (RSU) bands. Using the average received power at the selected bandwidths and knowledge of the locations of the base stations, a local ML-based algorithm estimates the path loss exponent and computes the approximate distance between the receiver and the corresponding transmitters. Applying simple multi-lateration techniques provides, with some uncertainty, the location of the vehicle relative to the transmitters and, subsequently, the global location of the vehicle.

2) Collaborative GPS location integrity check: We now introduce a collaborative approach for GPS integrity check, which exploits the CARAMEL infrastructure. Consider a vehicular network of \( N \) interconnected vehicles that are moving in the road network. The location of vehicle \( i \) at time \( t \) is denoted \( X_i^t = [x_i^t, y_i^t]^T \).

Based on [14], each vehicle at time \( t \) can collect three types of measurements: (i) absolute position measurement \( z_p^t \) from the GPS, (ii) relative distance measurement between neighboring vehicles \( z_d^{i,j} \) using LIDAR/RADAR, and (iii) relative azimuth angle or angle of arrival measurement between neighboring vehicles \( z_a^{i,j} \) using LIDAR/RADAR. The relative distance at time \( t \) between the neighboring vehicles \( i \) and \( j \) is modelled as \( z_d^{i,j} = \|X_i^t - X_j^t\|_2 + N_d \), where \( \|(.)\|_2 \) is the Euclidean distance and \( N_d \) is the measurement noise. The relative azimuth angle or angle of arrival at time \( t \) between neighboring vehicles \( i \) and \( j \) is modelled as \( z_a^{i,j} = \arctan(y_i^t - y_j^t)/(x_i^t - x_j^t) + N_a \), where \( N_a \) is the measurement noise. Obviously, \( z_p^0 \) is \( X_i^t + N_p \), where \( N_p \) is the GPS noise. The accuracy of the GPS, as well as the detection rate of possible location attacks, can be improved by fusing these measurements, which is known as the multimodal fusion method for cooperative localization.

All vehicles transmit their measurements, through CAM messages over their LTE-Uu interface, to an ITS application that runs in the MEC. In the MEC, the GPS is always assumed to be spoofed and the measurement model for the GPS is modified according to: \( \tilde{z}_p^t[i]^t = z_p^t[i]^t + o_p[i]^t \), where \( O_p \) is a sparse outlier matrix that models attacks. To this end, the following minimization problem is formulated, while the solution provides the estimated locations of the \( N \) vehicles:

\[
\begin{align*}
\arg\min_{X(t),O_p} & \sum_{i=1}^N \sum_{j=1}^{N(i)} (z_d[i,j]^t - \|X_i^t - X_j^t\|_2 )^2 \\
& + \sum_{i=1}^N \sum_{j=1}^{N(i)} (z_a[i,j]^t - \arctan(y_j^t - y_i^t)/(x_j^t - x_i^t) )^2 \\
& + \sum_{i=1}^N \|\tilde{z}_p[i]^t - o_p[i]^t\|_2 + \lambda \|O_p\|_1
\end{align*}
\]

To detect attacked vehicles, the estimated locations are compared against the respective GPS locations. If the difference exceeds a predefined threshold, then an attack is detected.

As a simple example, we consider a network of 20 moving vehicles/nodes for 100 time instances. Figure 4 depicts some preliminary results, where \( O_p \) is considered equal to 0 in Eq. 2 by the solver. The CDFs of the maximum GPS and cooperative location estimation errors are plotted at each time step with 0, 2 and 4 attacked vehicles/nodes, respectively. The attack is simulated by adding the maximum \( x \) and \( y \) coordinate of the vehicles to the attacked node(s). We observe that even in the attack-free case, the cooperative method attains lower localization error compared to GPS due to the additional inter-vehicle measurements. Importantly, in the event of location spoofing attack to 2 or 4 vehicles the proposed approach demonstrates remarkable robustness as the localization error is slightly increased, contrary to the GPS location error.
The CARAMEL project investigates advanced methods for the detection and mitigation of cybersecurity attacks in connected and autonomous vehicles. This work focuses on GPS location spoofing attacks that pose a serious threat to all involved actors including vehicles, infrastructure, drivers, pedestrians, etc. Two complementary approaches are proposed for detecting such attack and the development of a future feasible countermeasure, based on revoking the certificates of the attacked vehicles, is outlined.

As a future step, the overhead of CRLs distribution on the network traffic load, as well as scalability with regards to the number of attacked vehicles (and consequently the volume of revoked certificates) will be studied.

ACKNOWLEDGMENT

This work was supported by the European Union’s H2020 research and innovation programme under the CARAMEL project (Grant agreement No. 833611). The work of Christian Vitale, Christos Laoudias and Georgios Ellinas 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. The work of Jordi Casademont and Pouria 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.

REFERENCES

[1] R. Riebl, C. Obermaier, S. Neumeier, and C. Facchi, “Vanetza: Boosting research on inter-vehicle communication,” Proceedings of the 5th GI/ITG Fachgespräch Inter-Vehicle Communication (FG-IVC 2017), pp. 37–40, 2017.
[2] T. ETSI, “Etsi ts 102 941 v1. 3.1-intelligent transport systems (its); security; trust and privacy management,” standard, tc its, 2019.
[3] J. Cui, L. S. Liew, G. Sabalaiskaitė, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Networks, vol. 90, p. 101823, 2019.
[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” Vehicular Communications, vol. 1, no. 2, pp. 53–66, 2014.
[5] K. Deepa Thilak and A. Amuthan, “DoS attack on VANET routing and possible defending solutions-A survey,” 2016 International Conference on Information Communication and Embedded Systems, ICICES 2016, no. Icices, pp. 1–7, 2016.
[6] M. C. Chuang and J. F. Lee, “TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks,” IEEE Systems Journal, vol. 8, no. 3, pp. 749–758, 2014.
[7] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, “Djav: Detecting jamming attacks in vehicle ad hoc networks,” Performance Evaluation, vol. 87, pp. 47–59, 2015.
[8] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A security credential management system for V2V communications,” IEEE Vehicular Networking Conference, VNC, pp. 1–8, 2013.
[9] F. M. Salem, M. H. Ibrahim, and I. Ibrahim, “Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks,” in 2010 ICNS. IEEE, 2010, pp. 156–161.
[10] A. Wasef and X. S. Shen, “EMAP: Expedite message authentication protocol for vehicular ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2013.
[11] J. Li, H. Lu, and M. Guizani, “ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETS,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938–948, 2015.
[12] P. Gutierrez, “Galileo to transmit open service authentication,” Inside GNSS, 2020.
[13] N. Souli, P. Kotios, and G. Ellinas, “Relative positioning of autonomous systems using signals of opportunity,” in 2020 IEEE 91st Vehicular Technology Conference (VTC Spring). IEEE, 2020, p. to appear.
[14] H. Kim, S. H. Lee, and S. Kim, “Cooperative localization with distributed admn over 5g-based vanets,” in 2018 IEEE Wireless Communications and Networking Conference (WCNC), April 2018, pp. 1–5.