Grant Agreement No.: 814956
Research and Innovation action
Call Topic: ICT-22-2018 EU-China 5G Collaboration

5G HarmoniseD Research and TrIals for serVice Evolution between EU and China

D5.3: Final Report of Security and Data Protection in Future 5G Vehicular Networks

Version: 1.0

Deliverable type	R (Document, report)
Dissemination level	PU (Public)
Due date	31/05/2021
Submission date	27/10/2021
Lead editor	Adrian Quesada Rodriguez (MI)
Authors	Renáta Radócz (MI); Cédric Crettaz (MI); Abdelwahab Boualouache (Uni.lu); Ridha Soua (Uni.lu); Sébastien Ziegler (MI), Kinga Képessy (MI), Anna Kourakli (MI)
Reviewers	Sławomir Kukliński (Orange), Coen Bresser (ERTICO)
Work package, Task	WP 5, T5.4
Keywords	Privacy, Security, Personal Data Protection, 5G, Vehicular Networks

Abstract

This report will highlight the different challenges in terms of secure and privacy-friendly data communications in 5G future vehicular networks. It introduces a comprehensive assessment of the legal and standardization frameworks, and the key issues surrounding the topic, identifies a key set of requirements for personal data protection, and proposes novel technical and organizational solutions for ensuring security and privacy.

Document revision history

Version	Date	Description of change	List of contributor(s)
V0.1	02/12/2020	Draft final report generated based on intermediary report	Adrian Quesada Rodriguez
V0.2	01/02/2020	Update on legal state of the art and gap analysis	Anna Kourakli, Kinga Képessy
V0.5	12/02/2021	Unilu inputs (Sections 3.1.1, 3.1.2, and 3.1.3)	Abdelwahab Boualouache
V0.6	08/03/2021	Unilu inputs (Sections 3.1.4, 3.1.5, and 3.1.6)	Abdelwahab Boualouache
V0.7	22/04/2021	MI review and content unification	Adrian Quesada Rodriguez
V0.8	04/05/2021	Update following ENISA publication, format update and format/reference bug fixes	Anna Kourakli, Kinga Képessy, Cédric Crettaz, Renáta Radócz
V0.9	20/05/2021	Criteria finalization and internal review + Peer review submission	Adrian Quesada Rodriguez, Sébastien Ziegler, Renáta Radócz
V0.91	31/05/2021	Peer review inputs adopted, addresed comments and inputs from peer reviews	Slawomir Kukliński, Coen Bresser Adrian Quesada Rodriguez, Abdelwahab Boualouache, Sébastien Ziegler, Renáta Radócz
V0.92	02/06/2021	Final version generated and submitted to Coordinator	Adrian Quesada Rodriguez
V0.93	07/06/2021	Final editing, sent for GA approval	Anja Köhler
V1.0	26/10/2021	Enhanced Executive summary as requested by reviewers	Adrian Quesada Rodriguez

Disclaimer

This report contains material which is the copyright of certain 5G-DRIVE Consortium Parties and may not be reproduced or copied without permission.

All 5G-DRIVE Consortium Parties have agreed to publication of this report, the content of which is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License[1].

Neither the 5G-DRIVE Consortium Parties nor the European Commission warrant that the information contained in the Deliverable is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

Executive Summary

5G-DRIVE is an innovative Horizon 2020 project focused on harmonizing research and trials between the EU and China in the area of service evolution for 5G, and Vehicle-to-Everything (V2X). Deliverable 5.3 reports all results achieved from the research on security and personal data protection in future 5G vehicular networks.

As originally planned, Task 5.4 examined future security and personal data protection challenges in Internet of Vehicles (IoV) within the 5G ecosystem. To do so, the following actions were performed:

An analysis of the relevant legal frameworks was carried out and followed by an identification of relevant standards and the identification of the key personal data protection in V2X (legal and technical issues) and security requirements (by UN, EU-general, EU-ITS; China Cybersecurity Law). While the research identified several divergent elements in both the EU and Chienese approach, certification as a voluntary element has been showcased as a key commonality.

The multitude of reference sources and the great number of legal requirements involved generate obstacles to the interoperability and massification of V2X communications, as various jurisdictional requirements may present technical and organizational obstacles to the entry into the market of foreign solutions. A potential solution to this can, however, be found in voluntary GDPR-specific certification schemes, for example following the Europrivacy approach. Extensions related to V2X have been proposed.

Additionally, an overview of the international standards and recommendations has been performed (IEEE WAVE, ITU-T SG17, ISO/IEC and ETSI). Both these actions led to the identification of requirements and issues of relevance in the connected vehicle ecosystem, which could be tackled through either technical or organizational solutions. Furthermore, a high-level data protection assessment of the 5G-DRIVE trials was also performed to further enrich the identified context leading to the identification of potential areas of enhancement which have been addressed by the proposed technical solutions, namely:

1) Situation-centric and dynamic pseudonym changing strategy for SDN-based 5G Vehicular Networks: addressing the installation of the security parameters of the pseudonym changing strategy, local SDN monitoring (mobility, security parameters) and the pseudonym changing process, dynamic changing of the PCS security parameters and the update of the SDN controllers.
2) Privacy-by-design approach for SDN-based 5G Vehicular Networks: Detailing optimal placement of the Vehicular Location Privacy Zones (VLPZs) using genetic-based algorithm to ensure minimized trajectory cost of involved vehicles has been proposed. VLPZ consists of one entry point (router), one exit (aggregator) and a limited number of lanes. In the VLPZ, vehicles can change their pseudonyms in a secure way, they must change its pseudonym before leaving the VLPZ.
3) Situation-centric and dynamic misbehavior detection system (MDS) for SDN-based 5G Vehicular Networks: Exploiting SDN for a context-aware Misbehavior Detection Systems (MDS). Based on the context, the system can tune security parameters to provide accurate detection with low false positives. The system is Sybil attack-resistant and compliant with vehicular privacy standards. The simulation results show that, under different contexts, our system provides a high detection ratio and low false positives compared to a static MDS.
4) Blockchain for cooperative location privacy preservation in 5G-enabled vehicular fog computing: A monetary incentive scheme for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing. It leverages a blockchain-enabled fog with a resilient and lightweight consensus algorithm and smart contracts for cooperative Pseudonym Changing Processes (PCPs). The performance analysis confirmed effective incentive techniques non-cooperative vehicles, optimal monetary cost, and fast validation of blocks.
5) SDN-based privacy protection framework for 5G Vehicular Networks: an innovative software-

defined location privacy architecture for vehicular networks. The proposed architecture is context-aware, programmable, extensible, and able to encompass all existing and future pseudonym-changing strategies. To demonstrate the merit of the proposed architecture, a case study is considered that involves four pseudonym-changing strategies, which is deployed over the architecture and compared with their static implementations.

6) Blockchain-SDN based Architecture for 5G vehicular data trading: A scalable and secure data trading scheme for 5G-enabled Vehicular Fog Computing based on Software-Defined Networking (SDN) and blockchain. The building blocks of this scheme are: (i) a blockchain-based system consists of several SDN controllers, which use resilient and lightweight consensus protocol to ensure fast and reliable block mining and validation; (ii) a secure and fair data trading smart contract between data requesters (vehicles) and data providers (vehicles); (iii) a Stackelberg game model to ensure an incentivize and fair service pricing; and finally (iv) an SDN-based dynamic and context-aware fog placement integrating a genetic algorithm for ensuring high data throughput and low latency.

Table of Contents

List of Figures

List of Tables

Abbreviations

API	Application Programming Interface
BEREC	Body of European Regulators for Electronic Communications
BSM	Basic safety messages
CAC	Cyberspace Administration of China
C-ITS	Cooperative Intelligent Transport System
CPISS	Information Security Technology – Personal Information Security Specification Chinese Standard
CSL	Cybersecurity Law (of the People's Republic of China)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSRC	Dedicated Short Range Communication
DVB	Digital Video Broadcast
EC	European Commission
EDPB	European Data Protection Board
EECC	European Electronic Communications Code
eMBB	Enhanced Mobile Broadband
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunication Standards Institute
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRVA	Working Party on Connected Vehicles
HOA	Higher Order Ambisonics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IoV	Internet of Vehicles
ISMS	Information Security Management System
ITU	International Telecommunications Union
ITS	Intelligent Transportation Systems
LoA	Level of Assurance
MAC	Medium Access Control
NRA	National Regulatory Authority
PCS	Pseudonyms Changing Strategy
PDP	Personal Data Protection
PIPL	Draft of the Personal Information Protection Law

PRC	People’s Republic of China
PUI	Persistent Unique Identifier
PVS	Probe Vehicle System
RSDNC	RSU-SDN Controller
RSU	Road side Unit
SDN	Software Defined Networking
TARA	Technology Area Review Assessment
UNECE	United Nations Economic Commission for Europe
URLLC	Ultra-reliable lower-latency communication
V2N	Vehicle-to-Network
V2X	Vehicular-to-Everything
VLPZ	Vehicular Location Privacy Zone
VRU	Vulnerable Road Users
VSDNC	Vehicular-SDN Controller
WAVE	Wireless Access in Vehicular Environments

1 Introduction and Methodology

Modern vehicles are a marvel of engineering. Long has passed the time where an automobile was only a tool for transport, as the integration of the rapid technological developments has gradually converted them into mobile, interconnected computers capable not only of entertaining their passengers but also of understanding them and sharing critical information with other vehicles and things.

The European Data Protection Board (EDPB) defines a Connected Vehicle as a "*vehicle equipped with many electronic control units that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle*" (EDPB, 2020). Their integration and interactions are one of the domains of Cooperative Intelligent Transport Systems (C-ITS), a key strategic element for Europe that seeks the convergence of investments and regulatory frameworks across the EU to enable fast deployment of C-ITS in the near future. Various research-oriented actions have proposed methods to ensure the high-speed interconnection of vehicles. 5G-DRIVE is one of such actions, seeking to demonstrate the Vehicle to Everything (V2X) connectivity using 5G communications.

As vehicles become increasingly interconnected and aware of their passengers, the relevance of strong security and personal data protection safeguards become fundamental topics of discussion towards the protection and mitigation of risks for both end-users and data subjects. This document focuses on the work performed during the 5G-DRIVE project, particularly with respect to the research carried out regarding security and personal data protection in future 5G vehicular networks.

The methodology followed by this deliverable aims to meet two main objectives: 1) the identification of relevant personal data protection and security requirements in dissimilar legal frameworks (EU-China) and standards (ISO, ETSI, ITU, ECCP, etc.); and 2) the identification of innovative methods to address these requirements; and enable security and personal data protection oriented future 5G Vehicular Networks.

To this end, an analysis of the relevant legal frameworks was carried out and followed by an identification of relevant standards and the identification of the key personal data protection and security requirements. This action was focused on the identification of viable, interoperable and strong network-level oriented technical and organizational requirements in two main areas: regulatory compliance (with a focus on the organizational actions that will be necessary for an eventual deployment of a future 5G Vehicular Network), and V2X (in close alignment with 5G-DRIVE WP4). Afterwards, a set of technical and organizational solutions were examined as potentially viable for the development of secure and personal data protection enabled 5G Vehicular Networks.

As such, this Deliverable will begin by introducing some general considerations surrounding 5G vehicular networks from multiple angles, including regulatory context (mainly focusing on the European Union and China), as well as related global standards on connected vehicles management. Section 3 is dedicated to identifying requirements and analyzing potential solutions. It considers connected vehicles from the personal data protection point of view, providing a high-level data protection assessment of the actions undertaken in the 5G-DRIVE project. Additionally, Section 3 leverages on the work done by institutions and global organizations on the identification of issues and potential solutions related to vehicular networks for identifying potential technical and organizational solutions going beyond the state-of-the-art research to further address the intrinsic difficulties related to connectivity. Section 3.4 proposes an innovative SDN-based pseudonym changing strategy to support both infrastructure and infrastructure-less vehicular zones, while Section 3.5 explores the use of personal data protection certifications to address the lack of harmonization between various jurisdictions and standard requirements, analyzing the value-added contribution of the Europrivacy™/® Certification Scheme. As Europrivacy is a hybrid scheme able to certify the compliance of domain-specific technologies with GDPR, ISO standards and other national requirements, the following subsection (Section 3.5.1.2) introduces the proposed criteria for extension in relation to 5G and connected vehicular networks as a solution for bridging the harmonization gap mentioned above.

2 5G Vehicular Networks: General considerations, State-of-the-Art and Key Issue Identification

2.1 General considerations

5G-DRIVE is an innovative project focused on harmonizing research and trials between the EU and China on 5G usage for enhanced Mobile Broadband (eMBB) and Vehicle-to-Everything (V2X). This document focuses on the work performed with respect to the research carried out regarding security and data protection in future 5G vehicular networks.

The objectives of 5G-DRIVE include developing 5G technologies and services at pre-commercial testbeds and then demonstrating Internet-of-Vehicle (IoV) services using Vehicle-to-Network (V2N) and Vehicle-to-Vehicle (V2V) communications. 5G-DRIVE performed trial scenarios on four main pilot sites in the EU[2], namely 5GIC in the UK, Espoo in Finland, JRC at Ispra in Italy, and the Orange test site in Poland.

In this context, 5G-DRIVE Deliverable D4.3 "Report on potential vulnerabilities of V2X communications" identified potential security vulnerabilities and provided a detailed description of tests (including penetration tests) that will be implemented by the Project. It provided, amongst other elements, a set of security requirements relevant to connected vehicles and a taxonomy of security attacks, which were complemented with an outline of security standards[3] for ITS-G5 and C-V2X standards. Among the security requirements, the Deliverable identified the following items:

"Privacy: the protection of privacy is an important factor in public acceptance and the successful deployment of this V2X technology. Three classes of the privacy protection in V2X communication system can be distinguished: (i) the identifier privacy protection, (ii) the location privacy protection, and (iii) the protection of the data exchanged. The exchanged private data in the V2X communication system such as financial transactions and text chat conversations can easily be protected using encryption mechanisms. For this reason, the protection of the identity and the location are often considered as the primary concerns for a privacy-aware V2X communication system." (University of Luxembourg, 2019, p. 17).

Given the technical nature and focus on the security of the aforementioned deliverable, the scope of privacy protections in regard to V2X is understandably important. This, however, does not detract from the fact that, in the European and Chinese contexts alike, topics like V2X and 5G are subject to several types of regulatory requirements beyond those included in Deliverable 4.3, and for which both technical and organizational activities must be intertwined to ensure compliance.

In Europe, the General Data Protection Regulation (GDPR) has generated an interesting landscape for the integration of these two technologies in connected or smart vehicles. As stated further below, the European legal framework has included specific personal data protection requirements which extend to the use of innovative technologies such as V2X and 5G, and regulatory authorities and oversight bodies have expressly generated both legal requirements, guidelines, and best practices to address the potential risks these technologies generate vis-à-vis data subject rights. On the other hand, the Chinese approach has relied mostly on the specification of legal requirements and the

[2] For more details on the trials, see 5G-DRIVE Deliverables 3.3, 4.3 and 4.4

[3] "Standards: Security for preserving privacy and safety regulations serving ITS solutions is a key challenge to tackle when implementing new services based on V2X communications. Thereby, several standardisation organisations (ISO, CEN, ETSI, IEEE, etc.) all around the globe are working hard, in one hand, in solo standardising new research findings as part of technological innovations and, in another hand, joining these efforts harmonising similar technologies in order to offer transparent and interoperable solutions. These efforts led to the publication of valuable standards allowing the widespread deployment of V2X communications, others are under construction."(University of Luxembourg, 2019, p. 19)".

generation of standards. These two perspectives, and the potential solutions to be recommended in both contexts, will be considered by this Deliverable and summarized in the upcoming sections.

2.2 Personal Data Protection in V2X: Legal and Technical Background

2.2.1 United Nations

Legal and regulatory work for the realization of sustainable mobility and the introduction of autonomous vehicles is centralized at United Nations Economic Commission for Europe (UNECE). It hosts multilateral agreements and conventions ruling the requirements related to the use of these new technologies (e.g., safety measures, connectivity, cybersecurity, testing methods, and safe integration) while liaising with relevant stakeholders. The UNECE also hosts the intergovernmental platform of the World Forum for Harmonization of Vehicle Regulations that defines technical requirements in the automotive sector. The World Forum created a dedicated Working Party on Connected Vehicles (GRVA) in 2018, where countries from all over the globe participate to mobilize their expertise (UNECE, n.d.).

The UNECE started its work in 2014 and successfully amended the 1968 Vienna Convention on Road traffic to allow autonomous vehicles in traffic and removed the 10 km/h limitation for autonomous systems included in UN Regulation No. 79. (UNECE, n.d.). In June 2020, the UNECE published its proposal for two new UN Regulations on cybersecurity and software updates after recognizing the threatening nature of cyberattacks against vehicles. Both Regulations came into force in January 2021 (UNECE, 2020).

2.2.1.1 UN Regulation on Cybersecurity and Cyber Security Management Systems

This new Regulation provides a framework for the automotive sector, applying to cars, vans or buses that have an automated driving system equipped. The UNCECE puts in place processes for identifying cybersecurity risks, verifying that risks were properly managed, monitoring and analyzing attacks while assessing that the measures are effective to current threats. These processes are monitored and audited by national technical services or homologation authorities. Additionally, the Regulation defines certain requirements for manufactures that they must demonstrate before releasing their vehicle on the market. These include the application of a Cyber Security Management System, risk assessment analysis, mitigation measures for reducing risks, measures of detection of and protection against cyber threats, monitoring activities, and efficient reporting (UNECE, 2020).

2.2.1.2 UN Regulation on Software Updates and Software Updates Management Systems

This Regulation provides another framework for the automotive sector and applies to vehicles that permit software updates of cars, vans, or buses. The Regulation defines certain necessary processes to be put in place, including recording the hardware and software version relevant to the vehicle, identifying relevant software, interdependencies, and vehicle targets, as well as assessing the adequacy of software updates and their effect on safety. Vehicle owners must also be informed about any updates and there should be a documented proof of all the implemented actions. Just as with the Regulation on Cybersecurity and Cybersecurity Management Systems, the actions are audited by national technical services or homologation authorities. Furthermore, manufactures also demonstrate that they put in place a Software Update Management System, protecting SU delivery mechanism, ensuring integrity and authenticity before releasing their vehicle on the market. They must also protect the software identification number and ensure that it is readable from the vehicle. For Over-The-Air updates, manufacturers must execute updates sufficiently and safely, informing users about each update, as well as restore the functions if the update failed (UNECE, 2020).

2.2.2 The European Union

2.2.2.1 The General Data Protection Regulation (GDPR)

Regulation 679/2016 of the European Parliament (hereafter 'GDPR' or 'Regulation') is the most important regulatory framework of the European Union regarding personal data protection. The main objectives of the Regulations are to prevent discrepancy between the Member States of the European Union in terms of procedures and sanctions and to harmonize the regulation of personal data protection across the European Union. Considering 5G vehicular networks' capacity to exchange a huge amount of data in a short time span, this regulation shall be considered a stronghold to ensure the 5G-DRIVE project's compliance with personal data protection laws in the European Union.

The GDPR aims to protect the processing of personal data of natural persons and the free movement of data (GDPR, 2016 Art. 2(1)). The scope of the GDPR also reaches beyond the jurisdiction of the European Union. First of all, it applies to data processing operations which are performed by either a data controller or processor who are established in the European Union and secondly to data processing operations performed by a data controller or processor not established in the European Union when such processing activities relate to one of the following actions: "*a) the offering of good or services to data subjects in the European Union, irrespective of whether a payment of such data subject is required; b) the monitoring of data subjects' behaviour as far as their behaviour take place within the European Union; c) places where European Union Member States' law applies by virtue of public international law*" (GDPR, 2016, Art. 3).

The GDPR sets out nine key data protection principles (namely, the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitations, integrity and accountability), which not only give a summary of the essential requirements of the regulation but also provide an indispensable base when it comes to compliance (GDPR, 2016, Art. 5). The principles of fairness, transparency, explainability and accountability of data processing on the connected and automated vehicles are also provided - among others – by the recommendations of the expert group to the European Commission on the ethics of Connected and Automated Vehicles, issued in 2020 (*New Recommendations for a Safe and Ethical Transition towards Driverless Mobility*, n.d.). Moreover, the GDPR calls for the adoption of pseudonymized processing operations whenever possible in order to strengthen data subjects' privacy and the security of collected information.

According to the GDPR, consent - being the legal basis of data processing activities - must be given by the data subject. There are several requirements provided by the GDPR for consent to be valid, such as freely given, specific, informed and unambiguous. In addition, the GDPR further specifies the consent requirements for data processing operations related to minors and to the processing of special categories of data (Andrea Jellinek, 2019).

The GDPR provides a separate chapter on the rights of the individuals in order to give them more control over their personal data. This chapter specifies the right to access, rectification, erasure, restrict processing, data portability, object and last but not least, the right to not to be subject to a decision based solely on automated processing. On the other hand, there are specific obligations given to data controllers and processors to comply with the requirements, such as to adopt data protection by design and default approach, to keep records of their data processing activities and also to perform a Data Protection Impact Assessments of processing operations entailing high risks for the rights and freedoms of the data subjects. Restrictions are established for the transfer of personal data outside of the European Union and particularly to those countries which do not ensure appropriate safeguards for the protection of personal data (GDPR, 2016, Chapter III, IV).

2.2.2.2 The Directive on Privacy and Electronic Communication (ePrivacy Directive) and the European Union Regulation on Privacy of Electronic Communication (ePrivacy Regulation)

The ePrivacy Directive, soon to be replaced by the ePrivacy Regulation, is the reference legal framework for electronic communications. The objective of the Directive was to establish minimum requirements for security and confidentiality of communication, to protect traffic and location data and to enhance the fundamental rights and freedoms of individuals to private life in the electronic communications sector. There was an urgency to turn the Directive into regulation due to the technological evolutions and the entry into force of the GDPR. These developments should trigger the further harmonization of legal frameworks across the European Union, allowing the alignment of protection standards in the electronic communications domain with personal data protection measures included in the GDPR. The proposal for the ePrivacy Regulation aims to protect not only the privacy of data subjects but also their personal data processed in relation to electronic communications in accordance with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. With respect to the GDPR, the ePrivacy Regulation will be considered *lex specialis*, and it is expected to address further aspects of electronic communications networks which have the possibility to affect the rights and freedoms of data subjects. Considering the rapid emergence of new technologies and their need for the better protection of the confidentiality of communications, the ePrivacy Regulation should also provide for rules, for instance, in machine-to-machine (M2M) communication, so that devices will not be allowed to transfer personal data without prior consent or that it clarifies the limits of processing of massive amounts of metadata. Moreover, the ePrivacy Regulation should also introduce stricter rules on the disproportionate use of cookies, such as the possibility to set absolute restrictions for third parties to process cookies (Proposal for Regulation on Privacy and Electronic Communication, 2017; IONOS, 2020).

Nonetheless, the proposal of the ePrivacy Regulation does not include any specific provisions for data retention, which means that the Member States are free to have national data retention frameworks that provide, *inter alia*, for targeted retention measures. However, they must still comply with Union law, based on the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights of the European Union (IONOS, 2020).

As pointed out by EDPB, the adoption of the ePrivacy Regulation "*is necessary to ensure an equal level playing field for every provider and to ensure the confidentiality of electronic communications*" (Andrea Jellinek, 2019). It is therefore crucial that future cooperation between Europe and China on 5G vehicular networks considers the necessity to comply with a GDPR-like framework for electronic communication.

2.2.2.3 Directive on Security of Network and Information Systems (NIS Directive)

The NIS Directive (Directive (EU) 2016/1148), adopted by the European Parliament on 6 July 2016 and entered into force in August 2016, is the European Union's main regulatory framework on cybersecurity. According to the NIS Directive, appropriate measures should be adopted by the Member States in order to ensure the security of the European Union's cyberspace. The rules of the NIS Directive cover sectors in the economy and society, specifically those which rely on ICT systems. In this regard, businesses in these sectors that are identified by the Member States as operators of essential services are required to take appropriate security measures and to cooperate with national authorities for preserving the essential service (European Parliament, 2016, Recitals 4-6).

The purpose of the NIS Directive is to provide measures that should be implemented so that a universal level of security network and information systems can be achieved within the European Union. Security of network and information systems is defined as the ability to resist any action that affects the "*availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*" (European Parliament, 2016, Art. 4(2)). The NIS Directive applies to both digital service providers and operators of essential services. Digital service providers are covered by the NIS Directive once the Directive is implemented to the national law of the Member States. On the other hand, essential services are only covered by the scope of the NIS Directive upon designation as such by the respective Member State. In order to be considered essential, a service has to meet three cumulative criteria: "*a) being considered essential for the maintenance of critical societal and economic activities; b) being dependent upon network and information systems; c) an incident would have significant* *disruptive effects on the provision of that service*" (European Parliament, 2016, Art. 5(2)).

Concerning the transport sector, and particularly road transport, the list of sectors in Annex II of the NIS Directive, which guides the identification of essential services, includes road authorities responsible for traffic management control and operators of Intelligent Traffic Systems (ITS) (European Parliament, 2016, Annex II).

2.2.2.4 Revised Directive on Security of Network and Information Systems (NIS 2 Directive)

On 16 December 2020, the European Commission presented a new EU Cybersecurity Strategy and adopted a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). The new cybersecurity strategy strengthens the resilience of Europe when it comes to cyber threats and also ensures that all citizens and businesses have the possibility to take advantage of digital tools and services. In addition, it enables the EU to strengthen its leading role in international cyber rules and standards by intensifying collaboration around the world to promote a global, open, stable, and secure cyberspace based on the rule of law, human rights, fundamental freedoms, and democratic values. Following this, the NIS 2 would cover medium and large entities distinguished based on their criticality for the economy or society, responding to the growing number of threats emerging from digitalization and interconnectedness. It would not only strengthen security requirements for companies (e.g., supply chain security or reporting obligations) but would introduce stricter oversight and enforcement measures for national authorities with sanction schemes all over the European Union (European Commission, 2020).

Given the scope and purpose of the 5G-DRIVE project, compliance with the NIS Directive's obligations is crucial for the successful deployment of 5G vehicular networks. The threat of cyber-attacks on connected cars through other vehicles, cloud services, or road infrastructure can take various patterns from exploiting existing vulnerabilities to malware deployment or the use of a man-in-the-middle attack vie a mobile network/WiFi network (Huq et al., 2021). Following a harmonized EU Directive on cybersecurity measures aims at tackling the threat and risk of such attacks further ensures the adequate protection of personal data, as well as the general safety of the drivers.

2.2.2.5 European Union Directive on Intelligent Transport Systems (ITS Directive)

The ITS Directive (Directive 2010/40/EU), which was adopted to advance the distribution of innovative transportation technologies across Europe aims to establish ITS services with the possibility for Member States to freely decide on which systems they wish to invest in. One of the main objectives of the ITS Directive is to sponsor the necessary mechanisms to increase the deployment and use of continuous ITS services across the European Union (European Commission, 2019). In general, the purpose of this initiative was to create an enhanced way for the functioning of the road transport system and reduce the negative external effects of road transport. More specifically, the ITS Directive pursued interoperability and continuity of applications, systems and services; coordination and monitoring mechanisms between all ITS stakeholders; and establish solutions for liability issues (Article 11) and for sharing data that support ITS services in respect of the legislation on privacy and data protection (Article 10). However, based on the 2019 Evaluation Report released by the European Commission, the ITS Directive could not fully achieve the set objective due to the slow and fragmented deployment of ITS services (European Commission, 2019).

In March 2019, the European Commission submitted a proposal for an ITS Regulation which was rejected in July 2019 by the Council of Europe on behalf of the Member States. While it can be said that the idea of having an ITS Regulation remains on the Commission's agenda, it is not possible to foresee when further steps will be taken in this direction (European Commission, 2019). This Directive is of particular relevance to 5GDrive due to the use of applications and services provided by ITS, which include the processing of data such as road data, traffic data and travel data, all considered to be revealing relevant information about the data subjects.

2.2.2.6 Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)

The “eIDAS” Regulation was adopted by the European Union in 2014, which aim is to offer a comprehensive legal framework across the Member States for mutual recognition and interoperation of cross-border eID management, trust services and certificates (European Council, 2014, Recital 2). Since the GDPR repealed Directive 95/46/EC, all provisions of the eIDAS Regulation have to be interpreted and applied in accordance with the GDPR. Regarding 5G-DRIVE, the eIDAS Regulation is an important normative framework for providing secure and seamless electronic interactions between users of 5G vehicles, 5G service providers and public authorities. The eIDAS Regulation focuses on identification rather than authentication and specifies that its primary objective is the “unique identification” of a person (Tsakalakis et al., 2017, p. 33). The eIDAS Implementing Regulation 2015/1501 (R 2015/1501) clarifies that unanimous persons’ identification takes place by transmitting a minimum dataset which should include a Persistent Unique Identifier (PUI). Moreover, the eIDAS Regulation defines predetermined Level of Assurance (LoA) thresholds to guarantee the identity of services’ users. There are three LoA levels: “Low”, where evidence of identity is assumed to be valid (e.g. an account with a media service provider); “Substantial” where evidence has to be validated (e.g. services entailing online payments); “High” where evidence requires biometric validation (e.g. services linked to the use of electronic IDs) (Tsakalakis et al., 2017, p. 38).

Under the eIDAS Regulation, it is possible to identify five groups of requirements for considering electronic identification systems compliant with the eIDAS Regulation (Tsakalakis et al., 2017, p. 39):

- *Quality requirements*: This set of requirements drives the operations necessary to conduct identification and authentication processes. In this sense, eID systems’ purpose is to make electronic identification possible, while the identification means of a natural or legal person employed by an identification system should perform an authentication function.
- *Governance requirements:* This group details the conditions relating to the number and roles of actors involved in the process of eID provision to end-users.
- *Administrative requirements:* This set of requirements refers to the internal administration and management of eID providers. According to these prerequisites, eID services must provide specific information on their functioning, such as the description of the identification system, the liability regime and their rules of procedure.
- *Security requirements:* In this group, the eIDAS Regulation establishes the minimum technical and organizational measures that eID providers have to implement to ensure the security of their service. Notably, these measures must comply with international and European Union standards.
- *Liability requirements:* The last group includes requirements referring to the identification of the party liable in case of damage. This part covers the allocation of liability share in case of multiple parties accountable for a violation, as well as the allocation of the burden of proof.

An important aspect of the eIDAS Regulation with respect to the 5G-DRIVE project refers to the concept of “legal equivalence”. Through this concept, the eIDAS Regulation set rules for the recognition and equivalence of eIDs services offered in third countries in order to equate them to those offered in the European Union. In other words, “legal equivalence” is conceived as a prerequisite for granting specific legal effects to third countries’ eIDs. However, it has to be highlighted that the concept only applies to qualified trust services, excluding thus eID systems (Tsakalakis et al., 2017, p. 40). The eIDAS Regulation establishes three requirements for “legal equivalence”: a) there shall be an agreement between the European Union and the third country or international organization; b) the Trust Service Providers in the third country need to meet the requirements applicable to qualified Trust Services in the European Union, and c) the third country needs to recognize qualified trust services provided in the European Union as legally equivalent to trust services in the third country. Qualified trust service providers shall be audited. When there are indications that personal data has been violated, the supervisory body shall inform the data protection authorities of the results of its audits (Article 20).

In the context of the 5G-DRIVE project, the eIDAS regulation establishes a noteworthy legal framework. Mutual recognition of electronic identification and authentication is the key to successful data transfer. Considering that 5G cars will be in-movement connected devices, they will be interacting with many other connected subjects (V2V, V2I, V2U). These interactions with the surrounding environment require vehicular networks to enable safe and secure identification of vehicles in accordance with the rules established in the eIDAS Regulation and in compliance with data protection obligations.

2.2.2.7 Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code

The EU Directive 2018/1972, establishing the European Electronic Communications Code, lays down rules for regulating the electronic communications networks, telecommunications services and related facilities and services, while also establishing a set of procedures to ensure harmonization of the regulatory framework across the EU (European Parliament, 2018).

The European Electronic Communications Code (EECC), which entered into force in December 2018, is one of the main pillars of the EU Single Digital Market with the purpose to adapt EU legislation to current developments of communications. The EECC strengthens consumer rights and choice, for example, by ensuring clearer contracts, quality services and competitive markets. The code also ensures higher standards for communication services, including more efficient and accessible emergency communications. In addition, it enables operators to benefit from rules that provide incentives for investment in very high-capacity networks, as well as enhanced regulatory predictability, resulting in more innovative digital services and infrastructure (European Parliament, 2018).

The EECC is a key legislation to ensure the full participation of all EU citizens in the digital economy and in the European Gigabit Society. In order to assist the Member States in transposing the Directive into national law, the Commission has provided extensive guidance and assistance. In addition, the Body of European Regulators for Electronic Communications (BEREC) has developed and published guidelines aimed at the successful implementation of the new rules. BEREC assists the European Commission and the national regulatory authorities (NRAs) in ensuring the consistent implementation of the EU legislation by the Member States so that the EU has an effective internal market in the telecoms sector. In addition, the Commission, the BEREC and the authorities concerned shall ensure compliance of their processing of personal data with Union data protection rules (Article 1). In respect of the information exchanged, Union data protection rules shall apply (Article 11). The directive states that encryption should be mandatory in accordance with the principles of security and privacy by default and by design (European Parliament, 2018).

Of particular interest is recital 16 of the Directive in relation to the GDPR regarding electronic communications services which are provided to the end-user in exchange for the provision of personal data. As mentioned in the recital, in order to fall within the scope of the definition of electronic communications services, a service needs to be provided normally for a fee. In the digital economy, market participants increasingly believe that user information is of monetary value. Electronic communications services are often provided to the end-user for not only monetary consideration but more and more often for the provision of personal data or other data. The concept of remuneration should therefore cover situations where the service provider requests and the end-user knowingly provides personal data within the meaning of Regulation (EU) 2016/679 or other data directly or indirectly to the provider. It should also include situations in which the end-user allows access to information without actively providing it, such as personal data, including IP address or other automatically generated information, such as information collected and transmitted through cookies (European Parliament, 2018). Considering the aim of the 5G-DRIVE project, compliance with the European Electronic Communications Code is essential for a successful deployment of 5G vehicular networks, ensuring the protection of personal data, consumer rights and higher standards for communication services.

2.2.2.8 Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

The European Union set up a new institutional framework for cybersecurity, which not only strengthens the position of the EU Agency for Cybersecurity (hereafter 'ENISA') but also sets up a cybersecurity certification system for products and services. The Cybersecurity Act entered into force on 27 June 2019 is the first regulation of the European Union, which by increasing trust and security through specific cybersecurity criteria, will enable companies to have their ICT products, services and processes certified. The new certification system will make the recognition of these certificates possible in all Member States of the European Union (European Parliament, 2019).

The cybersecurity certification framework incorporates security features in the early stages of technical design and development and allows users to certify the level of security and ensures independent verification of these security features. The aim of these rules is to help build public confidence in the devices which are used on a daily basis, as there is a possibility to choose between products, such as IoT devices which provide a high level of safety in the cyberspace. This cybersecurity certification system will evaluate products and services and certify them when they meet specific criteria and rules (European Parliament, 2019).

The certification framework is a one-stop shop for the issuance of cybersecurity certifications. This will provide significant cost savings for businesses and especially for small and medium-sized enterprises, which would otherwise have to apply for various certifications in different countries.

2.2.3 China

2.2.3.1 The People's Republic of China Cybersecurity Law (CSL)

Implemented in 2017, the Cybersecurity Law (CSL) of the People's Republic of China (PRC) is the first regulation that addresses cybersecurity and protection of privacy on the national level. It reflects the PRC's view on cybersecurity and reveals an intent for building a robust information system that is resistant to threats. With the new CSL, China embraced its longstanding assertion of sovereignty over cyberspace for protecting and strengthening national security, while simultaneously enhancing internet surveillance for monitoring information flow and controlling foreign technologies. For this purpose, domestic internet operators and critical information infrastructures are regulated with specific provisions contained in the Cybersecurity Law. An example of such infrastructural measures adopted by China is the so-called "Great Firewall" that has effectively facilitated the implementation of the data localization requirement contained in the regulation (J.-A. Lee, 2018).

The key legal issues regulated by the CSL refer to: obligations of networks operators, defense of critical infrastructures, data localization requirements, security inspection and protection of personal information (Lee, 2018, p. 70). Regarding network operators, the law defines them as networks owners, managers, and service providers. The definition is broad and allows the application of network operators' obligation contained in the law to a wide range of actors. The main obligations of network operators are: "*a) formulate internal security management systems and operating rules, determine personnel responsible for network security and implement network security protection responsibilities; b) adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering network security; c) adopt technological measures for monitoring and recording network operational statuses and network security incidents and follow relevant provisions to store network logs for at least six months; d) adopt measures such as data classification, back-ups of important data, along with other obligations provided by law or administrative regulations*" (Creemers et al., 2018, Art. 21; Lee, 2018, p. 71) Interestingly, the Cybersecurity Law requires network operators to develop emergency response plans to react to cybersecurity incidents and, should any incident occur, they must implement remediation measures and report the incident to the authorities. If the network operator fails to fulfil any of these obligations, the competent authorities can order corrections and warnings. Authorities can also issue fines to network operators and management personnel directly responsible for the violation (Creemers et al., 2018).

The regulation uses the term “critical infrastructures” to refer to the facilities, systems and networks that are socially and economically crucial to the functioning of a country. The social and economic importance is determined upon considerations of national security, economic vitality and citizens’ health and safety. In this sense, the concept of critical infrastructures covers a wide variety of sectors, including transportation (Creemers et al., 2018; J.-A. Lee, 2018). According to the CSL, critical infrastructure is an infrastructure that might endanger national security, the welfare system, the people’s livelihood and the public interest if destroyed or rendered dysfunctional. In addition to this very broad definition, the State Council has the competence to define the scope of application and security measures of critical information infrastructures, leaving thus a great governmental discretion in this regard (Creemers et al., 2018).

Probably the most characterizing feature of the Cybersecurity Law is the data localization requirement. Data localization typically refers to policies requiring companies to store data regarding their users in servers within their jurisdictional borders. Under the Cybersecurity Law, operators of critical information infrastructures have to comply with an additional obligation regarding data localization requirements (Creemers et al., 2018, Art. 37). It is required to store personal information and “other important data” and its transfer, especially abroad, is subject to prior security assessment and authorization. Noncompliance with this obligation can result in a warning, service shutdown, license revocation or fines (Creemers et al., 2018; J.-A. Lee, 2018). Nevertheless, it is not defined in the regulation what constitutes “important data”.

The Cybersecurity Law also provides for a regime for certification, inspection, and review of cyberspace security measures. It stipulates that critical network equipment and specialized network security products “*shall follow the national standards and mandatory requirements with the security level certified by a qualified institute or confirmed by security inspection*” (Creemers et al., 2018). In this regard, network products and services that might affect national security have to sustain a national security review by the government.

The Cybersecurity Law also includes a section on personal data. The law defines “personal information” as information that can be used individually or jointly with other information to establish the identity of a natural person (J.-A. Lee, 2018). The definition covers, for example, a person’s name, birthday, ID number, biological identification information, address, and telephone number. On the other hand, when the information is de-identified, it is no longer subject to the Cybersecurity Law. The regulation stipulates that the collection and use of personal information by networks operators must be legal, proper and necessary (Creemers et al., 2018, Art. 43). It is also required that network operators disclose the purpose, method, and scope of their data collection and obtain the consent of the person whose personal information is collected. The CSL also establishes a prohibition of disclosure of collected personal information to any third party except when the relevant person gives their consent or the information has been processed in a manner so that the particular individual is unidentifiable and no recognizable information can be recovered (Creemers et al., 2018, Art. 42). In addition, under the Cybersecurity Law, personal information cannot be disclosed, altered, or destroyed by network operators. The limits on the use of personal information do not apply to the government, which, on the contrary, retains the power to control and survey personal information (J.-A. Lee, 2018). In this sense, network operators must support and assist public security authorities and the state security authority to protect national security and the investigation of crimes. Lastly, the Cybersecurity Law maintained the obligation for network operators to require users to disclose their real names and personal information and to deny provision of their services to those users who refuse to provide personal information (Creemers et al., 2018; J.-A. Lee, 2018).

2.2.3.2 Cyberspace Administration of China (CAC) Measures on Cybersecurity Review (Trial Measures)

Following Article 35 of the Cybersecurity Law, operators of critical information infrastructure must undergo a security review. China's national security is impacted by the procurement of networks products and services. In 2017, the Cyberspace Administration of China (CAC) released Measures on the Security Review of Network Products and Services (Trial) (hereinafter 'Trial Measures') to implement the above-mentioned requirement. The Trial Measures established processes for the CAC to conduct cybersecurity reviews. In 2019, a draft version of the Measures was released to the public, seeking comments for updating the review process of the Trial Measures. The final version of the draft was released in April 2020, under the name Measures on Cybersecurity Review (Measures) and took effect in June 2020 (Luo, Yan & Zhijing, 2020).

The Measures contains several obligations for operators of critical information infrastructure, including the "prediction" of potential national security risks associated with their procured products or services. If the operator identifies risk, it must apply for a cybersecurity review conducted by the Cybersecurity Review Office. Operators must also specify in their procurement agreements that providers of network products or services will assist such review. The Measures also defines the scope of network products and services that include the core network equipment, high-capability computers and servers, high-capacity data storage, large databases and applications, network security equipment, as well as cloud computing services. To oversee the various regulatory aspects contained, the Measures sets up a review body led by CAC and includes members of eleven governmental agencies, each of them assigned to a specific aspect (Luo, Yan & Zhijing, 2020).

2.2.3.3 Cyberspace Administration of China (CAC) Draft Measures for Data Security Management (Draft Data Security Measures)

In 2019, the Cyberspace Administration of China released the Measures for Data Security Management draft (Draft Data Security Measures) for public comments. Most requirements proposed by these Measures overlap with the Standardization Administration of China's national standard on personal information protection (see Section 2.2.3.8) (Luo et al., 2019a).

Summarizing the key provisions that overlap with the above-mentioned standard, the Draft Data Security Measures require network operators to publish privacy policies that include their rules for data collection and use (e.g., basic information of the network operator, purposes, types, volumes of data, security strategies implemented, etc.). Under the new Draft Measures, it is prohibited to force or mislead data subjects to consent to the collection of personal data through functions such as pre-checked authorization or bundled functions. Regarding data retention, data cannot be kept longer than it is described in the privacy policy of the network operator. Regarding network operators using personalized recommendations or targeted marketing, they must identify such information as "targeted push", providing a user-friendly opt-out mechanism. Before sharing personal information with third parties, network operators must assess the associated security risks and obtain consent. In case of a security incident, network operators must adopt remedial measures and notify their data subjects (Luo et al., 2019a).

There are also new requirements proposed, including the definition of important data as "*data that, if leaked, may directly affect China's national security, economic security, social stability, or public health and security*" (Luo et al., 2019a). If network operators collect important data, they must file their data collection practices with the CAC. However, the Draft Data Security Measures does not define the purpose and means of such a filing mechanism. Nonetheless, network operators must conduct a risk assessment of any handling of important data (e.g., publishing, sharing, cross-border transfer, etc.). Further concerning cross-border data transfers, they must obtain prior approval from their corresponding industry regulator or the CAC. Additionally, network operators must designate a person knowledgeable and experienced in data protection to oversee data protection efforts. Designated persons are responsible for coordinating the establishment and implementation of an internal data protection program, overseeing the completion of a DPIA, reporting on data protection practices and incident responses, and the handling of data subject complaints. The draft further defines potential penalties for network operators who failed to comply with the requirements (Luo et al., 2019a).

2.2.3.4 Cyberspace Administration of China (CAC) Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information (Draft Security Assessment Measures)

To further support the implementation of the Cybersecurity Law, the Cyberspace Administration of China released, along with the Draft Data Security Measures detailed above, the Measures for Security Assessment of Export of Personal Information draft for public consultation in 2019 (hereafter 'Draft Security Assessment Measures'). The main objective of the regulation is to put forward specific provisions related to the cross-border transfer or personal information. The Draft Security Assessment Measures extends the scope of the CSL, requiring all network operators to undergo a security assessment before handling personal information. Nevertheless, if other laws or regulations have already specified rules on cross-border data transfer of personal information, they must take precedence (Luo et al., 2019b).

As mentioned above, network operators are required to undergo a security assessment prior to data collection and transfer one time for each data recipient. On an ad-hoc basis or at least every two years, network operators must update their security assessment. Following Article 6, security assessments focus on key factors such as the compliance of the transfer with the applicable laws and regulations, the ability of contractual terms to protect the rights of personal information subjects, whether there is a history of harming legal rights and interests of personal information subjects and whether the obtaining of personal information is legitimate and lawful. After the applicable Provincial CAC has conducted the assessment, it sends back a report of results to both the operator and the central CAC (Luo et al., 2019b).

Furthermore, the Draft Security Assessment Measures also define the content of contracts between network operators and data recipients (Article 13), state the obligations of network operators (Article 14) and data recipients (Article 15). Particularly important for 5G-DRIVE, the draft also sets requirements for companies with no operation in China (Article 20). If an entity collects personal information in China but does not have any operations there, it must fulfil the same obligations imposed on network operators (Luo et al., 2019b)

2.2.3.5 Law of the PRC on the Protection of the Rights and Interests of Consumers (Consumer Protection Law)

The Consumer Protection Law entered into force in China in 1994 and was subsequently amended twice, in 2009 and 2013. This regulation represents the main legal framework for the protection of consumers' rights in China, as it establishes that consumers have the right to safety, choice, truthful information, fair treatment, to form social organizations and fair compensation (Jiang, 2019).

With the 2013 amendment, the regulation was updated to meet the increasing regulatory needs for the protection of consumers on the internet. The primary aim of the amendment was to extend to the digital market the safeguards already in place in the traditional economy. The law protects consumers' personal information and set rules for business operators. It requires providing explicitly the purpose, method, scope for collecting or using information and ensuring consumers' consent. Under the regulation, consumers' information is strictly confidential, and the law forbids business operators to disclose, sell, or provide illegally such information without consent. Companies have an obligation to remedy data loss and violations can result in fines or license suspension or revocation (Jiang, 2019).

Related to the Consumer Protection Law, brief mention must be given to the Advertising Law that defines internet advertising while establishing rules for publishers of online advertisements. The Advertising Law also defines the applicable controls and fines, dating back to 1994 (*Advertising Law of the People's Republic of China*, 1994).

2.2.3.6 Draft of the Personal Information Protection Law (PIPL Draft)

In October of 2020, China published a draft of the Personal Information Protection Law (PIPL Draft) with a month-long public comment period. The Draft, if passed, would become China's first comprehensive law on personal data protection. Much like the GDPR, the PIPL Draft distinguishes the principles of transparency, accountability, fairness, purpose limitation, data minimization, data retention, and accuracy. It also provides management and security measures in the form of compliance audits, risk assessments or data breach reporting. The PIPL Draft defines data subjects' rights, such as the right to information and explanation on data processing, access to the copy of personal data stored, right to correction, object processing, right to withdraw consent, or right to deletion (Creemers et al., 2020).

Article 4 states that personal information refers to "*all kinds of information recorded by electronic or other means related to identified or identifiable natural persons, not including information after anonymization handling*" (Creemers et al., 2020). Activities such as collection, storage, use, processing of personal information fall into the meaning of the handling of personal information. Organizations and individuals that handle such activities are referred to as personal information handlers and, according to Article 9, are required to follow safeguards to secure the personal information they handle (Creemers et al., 2020). The organization or individual who controls and determines the usage of personal data is referred to as a "data processor", without any differentiation from "data controller" as provided by the GDPR.

The Draft states certain circumstances under which the handling of personal information is allowed without consent. Such circumstances include public interest, protection of life, health or property, and other emergency situations and circumstances. Individual's consent must be given voluntarily and explicitly, with the full knowledge on personal information handling (e.g., including information on the identity, use, purpose, storage period, etc.). If personal information is provided to a third party, handlers must bring this information to the knowledge of the data subject and should obtain separate consent. Similar provisions apply if personal information is provided outside of PRC (Creemers et al., 2020).

In contrast to the Cybersecurity Law, which provides limited extraterritorial application, the PIPL Draft puts forward an overseas extraterritorial application to individuals and entities that handle personal information. Unlike in the GDPR, there are no provisions for adequacy determinations in third countries. While the GDPR promotes the free flow of data across borders providing for transfer mechanisms, the draft PIPL requires security assessments in case of abroad personal data transfer. Generally, the Draft provides for more expansive data localization requirements and states clearer rules on cross-border transfer of personal data (Creemers et al., 2020). This is an especially important piece to note for the 5G-DRIVE project for the harmonization and correct implementation of services.

2.2.3.7 Data Security Law of the People's Republic of China

In 2020, the Chinese government released a draft Data Security Law for public comment. Together with the Personal Information Protection Law, the Data Security Law is set to lay down new power and responsibilities for government bodies and private actors (Rafaelof et al., 2020).

The Draft law is presented in seven chapters. Few of the particularly notable provisions include Article 2 that defines the scope of the law beyond the borders of the PRC, stating that "*(w)here organizations or individuals outside of the mainland territory of the People's Republic of China engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations of the People's Republic of China, legal liability will be investigated according to the law*". Article 19 proposes a grading and classification system for differentiating the degree of impact on national security, public interest, the interest of citizens, etc. Furthermore, Article 25 calls for the establishment of a data security management system for those who conduct data activities. Article 3 defines data activities as "*data collection, storage, processing, use, provision, transaction, publication, and other activities*" while data security is understood as "*ability to adopt necessary* *measures to ensure data is effectively protected and lawfully used and remains continually secure in the state*" (Rafaelof et al., 2020).

2.2.3.8 Chinese Standard: Information Security Technology – Personal Information Security Specification GB/T 35273-2017 (CPISS)

The Chinese Standard: Information Security Technology – Personal Information Security Specification (CPISS) is a legal document complementing and clarifying existing data protection laws. It was adopted in 2017 by China's Information Security Standardization Technical Committee. With the introduction of this standard, China establishes a voluntary framework detailing the best practices for compliance with China's data protection laws. In many respects, this standard creates a system that is aligned with the GDPR. In other words, this document is an instrument of soft law but, although not mandatory, it is highly regarded when Chinese authorities review the conduct of personal information controllers (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

The CPISS applies to personal information controllers, including any private or public organization that has "*the power to decide the purpose and method*" of processing personal information (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017). The standard uses the term "personal information" to define the information that can be used to identify a specific natural person and not "personal data" as the GDPR does. The CPISS also provides rules for processing sensitive personal information. However, the standard's definition of sensitive personal information takes a different approach than the GDPR, for instance. The standard links the "sensitivity" of the information to the consequences, damages, and harm that a person might suffer if the information is lost, misused, or if it is capable of endangering persons, properties, or health, or if it may result in discriminatory treatment. For example, according to the context of the data processing activities, national identification card numbers, login credentials, GPS locations can amount to sensitive personal information (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

The CPISS adopts general principles that can be found in most data protection laws. The purpose for processing personal information must be clear, determined, and fair. Collection and processing of personal information should be proportionate, secure, based on a risk assessment approach and in compliance with the rights of individuals to control processing operation in relation to their personal information. Processing of personal information must be based on consent or on a limited set of exceptions that mirror the exception contained in the GDPR with some distinctions. According to the CPISS, consent to collect and process personal information is not necessary when:

- the personal information is directly related to national security and national defense, or directly related with public security, public health or major public interests;
- personal information is directly related to a criminal investigation, prosecution, trial, judgement, or enforcement;
- the purpose for processing is to defend material legal rights of personal information subject or other individuals;
- the personal information collected is disclosed by the personal information subject to the public; the personal information is collected from lawfully disclosed information;
- required for the execution or performance of a contract;
- the personal information is required to maintain the safe and stable operation of the product or service provided;
- the controller of the personal information is a news agency;
- the controller of the personal information is an academic research institution, and collection

and use are necessary for statistic or academic research for the public interest;

- in the presence of other circumstances stipulated by laws and regulations (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017, para. 5.4).

Notably, the standard does not mention "necessity for the legitimate interest of the controller or a third party" as an exception to lawful data processing absent consent. However, since the standard includes several exceptions to consent, it is possible to suggest that the legitimate interests of controllers can be considered mostly covered within these additional exceptions.

In principle, personal information has to be deidentified upon collection and the information necessary to re-identify anonymized personal information must be kept separated. To this end, the standards mandate that personal information controllers have in place adequate organizational measures to achieve this purpose (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017, para. 6.2).

Like the GDPR, the CPISS includes a purpose limitation requirement. Secondary use of collected information must relate to the original purpose for collecting the personal information. Additionally, the standard vests personal information subjects with several rights that mainly match the rights conferred to data subjects by the GDPR (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017, para. 7). Personal information subjects benefit from a strengthened right to erasure since the standard does not conceive exceptions to it and includes the controllers' obligation to notify third parties of the erasure. On the other hand, this right can be invoked only when such processing operations are in breach of any law or prior agreement with the personal information subject. Personal information subjects also have the right to have their accounts cancelled immediately if they so request. In general, the time limit to comply with the personal information subject's request is 30 days. The right to data portability is limited to a certain type of personal information such as health, education and occupational information (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

When a personal information controller intends to rely on a data processor, the CPISS requires the performance of a risk assessment to ensure adequate security of the process. Data processors always remain under the supervision of personal information controllers through audits and compliance assessments. When a data processor desires to contract a sub-processor, it may do so only with the data controller's permission. Processors share with the controller the obligation to comply with data subjects' requests and must notify the data controller in case of security incidents. In addition, processors are required to notify controllers when they cannot offer an adequate security level to personal information or when they need to process personal information outside the agreement with the controller (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

In accordance with the Cybersecurity Law, prior notice and consent from personal information subjects are necessary when non-de-identified personal data must be shared or transferred. The CPISS also suggests that in this circumstance, the transfer or sharing of personal information undergo a prior risk assessment and mitigation exercise. The standard also sets out specific records-keeping obligations regarding the sharing or transfer of personal information and an obligation on controllers to bear responsibility for any damage caused to individuals by the transfer or sharing of their personal information. In addition to the requirements set by the CPISS, share or transfer data also have to comply with the security assessment measures established by the Cyberspace Administration of China (People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

In terms of organizational measures, the standard requires controllers to:

- have internal procedures to grant access to personal information and authorize operations;

- keep records of data processing;
- put in place procedures for deidentification of data subject upon collection of personal information;
- appoint Chief Information Security Officer and designated personnel with responsibility for information security;
- conduct periodic staff training;
- conduct security training before the release of products or services;
- and have a dedicated security team if the controller’s organization meets a size threshold or process personal information of more than 500.000 personal information subjects.

Personnel with access to sensitive personal information must be subjected to background checks (People’s Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration, 2017).

2.2.4 Regulations - Summary matrix

UN Regulations	Key points	Application and relation to other laws
UN Regulation on Cybersecurity and Cyber Security Management Systems	• It applies to the automotive sector for vehicles that permit software updates. • Provides a framework for setting up a Cybersecurity Management System. • Defines rules for manufactures to follow before releasing their vehicle to the market.	Most recent UN-level Regulations defining a framework for cybersecurity and software updates in the automotive sector.
UN Regulation on Software Updates and Software Updates Management Systems	• It applies to the automotive sector for vehicles with an automated driving system equipped. • Provides a framework for setting up a Software Update Management System. • Defines rules for manufactures to follow before releasing their vehicle to the market.	

Table 1: UN regulation summary matrix

EU Regulations	Key points	Application and relation to other laws
The General Data Protection Regulation (GDPR)	It sets: • rules for free movement of data. • requirements for consent and the rights of data subjects. • obligations of data controllers, Data Protection by Design and by Default approach, DPIA etc. • a voluntary data protection certification (art. 42). system to demonstrate compliance	The main European Union regulatory framework in the field of personal data protection. Intrinsically related to the ePrivacy Regulation.

EU Regulations	Key points	Application and relation to other laws
The Directive on Privacy and Electronic Communication (ePrivacy Directive) and the European Union Regulation on Privacy of Electronic Communication (ePrivacy Regulation)	It provides for: • requirements for security and confidentiality of communication, protection of traffic and location data and protection of the end-user terminal equipment. • fundamental rights and freedoms, as the respect for private life in the electronic communications sector.	With respect to the GDPR, the ePrivacy Regulation will be considered *lex specialis*. Addresses further aspects of electronic communications networks that may affect the rights and freedoms of data subjects. It does not include any specific provisions for data retention.
Directive on Security of Network and Information Systems (NIS Directive)	• It is a legislation on cybersecurity, measures to guarantee the security of the European Union's cyberspace.	Digital service providers are covered by the NIS Directive regime upon the sole transposition of the directive into Member States' national law. Essential services are only covered by the scope of the NIS Directive upon designation as such by the respective Member State.
Revised Directive on Security of Network and Information Systems (NIS 2 Directive)	• It strengthens Europe's collective resilience to cyber threats. • It ensures that all citizens and businesses can take full advantage of reliable services and reliable digital tools. • It aims to address existing and future cyber and non-cyber threats.	The revised NIS presents a new EU cybersecurity strategy for shaping Europe's digital future. The EU Cybersecurity Act has equipped Europe with a framework for cybersecurity certification of products, services and processes and strengthened the mandate of the EU Agency for Cybersecurity (ENISA).
Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)	• It provides for mutual recognition and interoperation of cross-border eID management, trust services and certificates. • Its primary objective is the 'unique identification' of a person. • It defines predetermined Level of Assurance. • It clarifies that unanimous persons' identification	Since the GDPR repealed Directive 95/46/EC, all provisions of the eIDAS Regulation have to be interpreted and applied in accordance with the GDPR.

EU Regulations	Key points	Application and relation to other laws
	takes place by transmitting a minimum dataset which should include a Persistent Unique Identifier. • It sets requirements for considering electronic identification systems compliant.	
Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code	• It rules for the regulation of electronic communications networks, telecommunications services and related facilities and services.	It is without prejudice to measures taken at the Union or national level, in accordance with Union law, relating to the protection of personal data and privacy. In respect of the information exchanged, Union data protection rules shall apply (Article 11). Encryption should be mandatory in accordance with the principles of security and privacy by default and by design.
Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (Cybersecurity Act)	• It introduces a European cybersecurity certification system. • The system ensures that certified products, processes and services meet specific cybersecurity criteria.	The first EU Regulation to meet the security challenges of connected products, Internet of Things (IoT) devices and critical infrastructure through such certificates.

Table 2: EU regulation summary matrix

Chinese Regulations	Key points	Application and relation to other laws
The People's Republic of China Cybersecurity law (Cybersecurity Law)	• Cybersecurity and protection of privacy. • Internet surveillance for national security purposes. • Obligations of networks operators, defense of critical infrastructures, data localization requirements, security inspection and protection of personal information.	These provisions have been implemented by the Cyberspace Administration of China.

EU Regulations	Key points	Application and relation to other laws
Cyberspace Administration of China Measures on Cybersecurity Review	• Contains the obligations of operators of critical information infrastructure. • Defines the scope of network products and services that include the core network equipment, high-capability computers and servers, high-capacity data storage, large databases and applications, network security equipment, as well as cloud computing services. • Sets up a review body with the lead of the CAC.	Following Article 35 of the Cybersecurity Law, operators of critical information infrastructure must undergo a security review China's national security is impacted by the procurement of networks products and services; the Measures on Cybersecurity Review intends to further define the means of doing so.
Cyberspace Administration of China Draft Measures for Data Security Management	• Provisions in relation to data collection, retention and consent. • Defines important data and sets specific obligations in relation to its collection.	The Draft Measures provide detailed guidelines on how the security assessments should be operated and is intended to complement the Cybersecurity Law of China.
Cyberspace Administration of China Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information	• Procedure to export personal information outside China's cyber-jurisdiction. • The contract between the network operator exporting personal information and the foreign data recipient can be compared to a data transfer agreement or to the binding corporate rules of the GDPR.	
Law of the PRC on the Protection of the Rights and Interests of Consumers (Consumer Protection Law)	• Consumers have the right to safety, choice, truthful information, fair treatment, to form social organizations and fair compensation. • Protects consumers' personal information and sets rules for business operators. • Requires providing explicitly the purpose, method, scope for collecting or using information	The Advertising Law is another legislation that is related to the Consumer Protection Law. The definitions of advertisement and advertisement publishers are very broad and cover almost any sort of product or service promotion.

EU Regulations	Key points	Application and relation to other laws
	and ensuring consumers' consent.	
Draft of the Personal Information Protection Law (PIPL Draft)	• China's first comprehensive law on personal data protection. • Transparency, accountability, fairness, purpose limitation, data minimization, data retention and accuracy, principles provided by the draft PIPL (similar to GDPR principles). • Management and security measures (through compliance audits, risk assessments, data breach reporting and more) as in GDPR.	It is broader than GDPR, as personal information also refers to financial account information and the location of the individual. Narrower than GDPR, as it leaves out of the scope of the definition of personal information the trade union membership, political opinions, genetic and biometric data and information related to sexual life. In contrast to PRC Cyber Security Law, it puts forward an overseas extraterritorial application to individuals and entities. Unlike the GDPR, there are no provisions for adequacy determinations in third countries. In contrast to GDPR, it requires security assessments in case of abroad personal data transfer. More expansive data localization requirements and clearer rules on cross-border transfer of personal data.
Data Security Law of the People's Republic of China (Draft)	• Required steps to ensure data security is reached.	New power and responsibilities for government bodies and private actors, together with the Personal Information Protection Law.
Chinese Standard: Information Security Technology – Personal Information Security Specification GB/T 35273-2017 (CPISS)	• A voluntary framework detailing the best practices for compliance with China's data protection laws.	It creates a voluntary system that is aligned with the GDPR. It adopts general principles that can be found in most data protection laws. Establishes several rights to match the rights conferred to data subjects by the GDPR and includes a purpose limitation requirement. In accordance with the Cybersecurity Law, prior notice and consent from personal information subjects is necessary when non-de-identified personal data must be shared or transferred. Key reference when considering potential applicability of certification solutions for international data transfers.

Table 3: Chinese regulation summary matrix

2.2.5 EU-Chinese perspective comparison

The following table will provide a brief comparison of both the EU and Chinese perspectives, leveraging on the GDPR, the CSL and the CPISS. Although started the implementation of personal data protection measures later than the EU, both the Chinese Cybersecurity Law and the Chinese Standard show convergence with the EU law.

The EU General Data Protection Regulation	The People's Republic of China Cybersecurity law & Chinese Standard: Information Security Technology – Personal Information Security Specification
• Uses the definition of personal data and data subjects • Prior notice and consent (different legal bases for the processing of personal data) • Emphasis on data controllers and data processors • Data breach notification requirement to the supervisory authority and/or data subject • Independent Supervisory Authorities • Limiting further processing • Strong data minimization requirement • Specific requirements for sensitive data (e.g. biometric data, religious beliefs, genetic data, ethnicity, etc.) • Right to be forgotten is strongly enforced • Right to data portability • Personal data protection given human right level • High level of requirements for international data transfers • Voluntary certification system	• Used the definition personal information and personal information subjects • Prior notice and consent (lighter rules and does not require implicit consent) • Emphasis on network operators' obligations • Data breach notification requirement to authorities and data subjects but does not specify the timeframe or information • There are no specific supervisory authorities set up, however, the Cyberspace Administration of China handles enforcement efforts regionally • Limiting further processing • Softer data minimization requirement • Specific requirements for sensitive data but different definition (broader, risk-based definition) • Right to be forgotten is limited to specific cases • Right to data portability • No privacy-related restrictions for the generation of solutions • Conceptualized as national security • Voluntary certification system

Table 4: EU-Chinese perspective comparison

2.2.6 International Standards and Recommendations

2.2.6.1 IEEE 1609 Wireless Access in Vehicular Environment (WAVE) Working Group Standards Family

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest association of technical professionals for electronic and electrical engineering (*About IEEE*, n.d.). Its IEEE P1609 Working Group is responsible for defining the 1609 Family of Standards for Wireless Access in Vehicular Environment (WAVE), standardizing not only the architecture but the set of services and interfaces enabling secure wireless communications in vehicular environment (Ahmed et al., 2013). As of today, the IEEE 1609 family includes the following standards:

IEEE 1609.0-2019

This standard is used within architectures, describing the necessary architecture and service for multi-channel WAVE devices communicating in a vehicular environment ("IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture," 2019).

IEEE 1609.2-2016 (1609.2a-2017 and 1609.2b-2018)

This standard is used in security services for the applications and management messages, covering the methods for formatting secure management and application messages ("IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," 2016).

IEEE P1609.2.1-2020

This standard is used for end entities (e.g., entities who use digital certificates for the authorization of application activities) and includes certificate management protocols supporting the provisioning and management of digital certificates (*IEEE 1609.2.1-2020 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Certificate Management Interfaces for End Entities*, n.d.).

IEEE 1609.3-2020

This standard is used for networking services and describes those standard messages necessary for the support of higher layer communication stacks (*IEEE 1609.3-2020 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Networking*, n.d.).

IEEE 1609.4-2016

This standard is used for supporting multi-channel wireless operations by describing standard message formats [medium access control (MAC) layer] for interoperable and remote management of WAVE (*IEEE 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation*, n.d.).

IEEE 1609.11-2010

This standard is used for over-the-air electronic payment data exchange protocol, defining a basic level of technical interoperability for electronic payment equipment (e.g., onboard unit or roadside unit) by using Dedicated Short Range Communication (DSRC) ("IEEE Standard for Wireless Access in Vehicular Environments (WAVE)– Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)," 2011).

IEEE 1609.12-2019

This standard is used for identifier allocations for WAVE (*IEEE 1609.12-2019 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Identifiers*, n.d.).

The IEEE 1609 family of standards is particularly relevant for 5G-DRIVE as they concern the safety, security, and privacy of connected vehicles. For the successful deployment of devices, appropriate safeguards must be ensured by the application of such standards, securing communication in vehicular networks against threats.

2.2.6.2 ITU-T SG 17 Recommendations

The International Telecommunication Union (ITU) launched Study Group 17 (SG17) to promote and produce standardization recommendations on communication technology. ITS standardization research started in 2014 and is still ongoing. Currently, there are several ITU working groups developing recommendations on security aspects for ITS (S.-W. Lee et al., 2017; Schmittner & Macher, 2019). The following recommendations were identified as relevant for 5G-DRIVE:

X.1371 – Security threats to connected vehicles

This recommendation, published in 2020, lists security threats to connected vehicles and the vehicle ecosystem. The recommendation lists threats to be used for future standards as a reference, including threats related to backend servers, communication channels, update procedures, unintended human actions, and external connectivity. X.1371 also includes crucial information based on what can be a potential reason behind an attack, listing potential vulnerabilities (*X.1371: Security Threats to Connected Vehicles*, 2020). This recommendation is particularly useful as a baseline document for identifying threats and vulnerabilities, providing a great starting point for 5G-DRIVE in the identification of solutions.

X.1372 – Security guidelines for vehicle-to-everything (V2X) communication

This recommendation, published in early 2020, consists of guidelines for establishing safeguards in V2X communication systems. In the document, threats and security requirements for V2X communication systems are thoroughly analyzed. To this end, a basic model and use cases are presented in the standard. Then, an overview of the performance of a Technology Area Review Assessment (TARA) is presented together with the identification of necessary security requirements. Overall, the security requirements presented in X.1372 are based on the analysis of detected threats. In this sense, the recommendation defines several attacks relating to several aspects of V2X communication such as vehicle and RSU authentication, integrity and confidentiality of messages, privacy, and suspicious behavior of the onboard unit (*X.1372: Security Guidelines for Vehicle-to-Everything (V2X) Communication*, 2020).

X.1373 - Secure software update capability for intelligent transportation system communication devices

This recommendation, published in 2017, focuses on secure software updates for ITS communication devices. The main objective of this recommendation is the prevention of threats, providing guidance against several risks that may affect communication devices on vehicles. This recommendation contains a basic model of software updates, introducing a method to analyze threats and risks for software updates and provides security requirements accordingly. In addition, it specifies modules for software update through an abstract data format (*X.1373 : Secure Software Update Capability for Intelligent Transportation System Communication Devices*, 2017).

X.1374 - Security requirements for external interfaces and devices with vehicle access capability

The main goal of this recommendation, published in late 2020, is to identify security issues when external devices, either with or without a telecommunication interface, are connected to the On-Board Diagnostic Port and defines suitable security requirements to protect this external interface. The recommendation specifies requirements for external interfaces and devices with vehicle access capability in telecommunication network environments, addressing identified threats (*X.1374 : Security Requirements for External Interfaces and Devices with Vehicle Access Capability*, 2020).

X.1375 - Guidelines for an intrusion detection system for in-vehicle networks

The main purpose of this recommendation, published in late 2020, is to provide comprehensive guidance on the identification of intrusions in the system. In this document, the ITU SG17 classifies and analyses typical attacks on in-vehicles networks and systems. In particular, it focuses on in-vehicle networks which general Intrusion Detection Systems (IDS) cannot support (e.g., CAN or CAN-FD) (*X.1375 : Guidelines for an Intrusion Detection System for in-Vehicle Networks*, 2020).

X.1376 - Security-related misbehaviour detection mechanism using big data for connected vehicles

This recommendation, published earlier this year, describes a misbehavior detection mechanism for connected vehicles in two steps: 1) data capture that specifies the types of data captured from different sources to detect misbehavior; 2) detection that analyzes captured data (*X.1376 : Security-Related Misbehaviour Detection Mechanism Using Big Data for Connected Vehicles*, 2021).

As mentioned above, the recommendations of ITU-T on connected vehicles provide guidelines for not only identifying threats to connected vehicular networks but introduce effective measures on tackling such threats and risks.

2.2.6.3 ISO/IEC 27000:2018 – Information Security Management System (ISMS) family of standards

Management system models standards by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provide a setting for operating management systems. The Information Security Management System (ISMS) family of standards provides a framework for organizations to manage the security of their assets, information, or intellectual property under over 19 standards (*ISO/IEC 27000:2018(En), Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*, n.d.). The following standards were identified as especially relevant for 5G-DRIVE to ensure the security of connected vehicular networks:

ISO/IEC 27001:2013 Information Security Management (ISO 27001)

ISO/IEC 27001:2013 is an international standard designed to establish an information security management system within an organization. Overall, the standard requires monitoring the risks to information security in an organization and examine possible threats and vulnerabilities. In case of identification of any risk, the standard calls for the implementation of an appropriate form of risk treatment to reduce the risk to an acceptable risk. The standard also requires that the management of information security follows a process that ensures that the organization's information security needs are met on an ongoing basis. ISO 27001 has been construed to be technology-neutral and to follow a top-down risk-based approach. The document defines a process divided into different parts: define a security policy; define the scope of the information security management system; conduct a risk assessment; manage identified risks; identify control objectives and controls to implement; prepare a statement of applicability (International Organization for Standardization, 2013a).

The standard requires that all sections and branches of the organization cooperate in implementing and respecting the standard. Among the specifications provided, ISO 27001 includes details for documentation, management responsibility, internal audits, continual improvement and corrective and preventive actions (International Organization for Standardization, 2013a).

It is necessary to note that ISO 27001 does not require the use of specific information security controls but provides a checklist of controls that should be considered in the accompanying code of practice. In the code of practice, it is described a set of objectives and good practice to achieve control of the information security management system that is efficient and effective.

ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls (ISO 27002)

ISO/IEC 27002:2013 intends to guide the adoption of information management security standards and information security management practices. The scope of this technical report includes selection, implementation and management of controls suitable to establish an information security system. In guiding the user through the adoption of the most suitable measures, the standard considers the risks arising from the environment in which the organization operates (International Organization for Standardization, 2013b).

The standard is directed to organizations that: "*select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines*" (International Organization for Standardization, 2013, para. 1).

ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management (ISO 27005)

ISO/IEC 27005:2018 is an international standard based on a risk management approach. ISO 27005 describes the process of information security risk management. This process is composed of different activities: establishment of the risk management context; assessment of the relevant information risks; handling of the risks; information to the stakeholders; as well as monitoring and review of the risks. This is a continuous process that should be done regularly. The appendices of the ISO 27005 standard provide examples of how to implement the risk management approach described in the body of the standard (*ISO/IEC 27005:2018(En), Information Technology — Security Techniques — Information Security Risk Management*, 2018).

ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines (ISO 27701)

ISO/IEC 27701:2019 is an international standard aiming to provide specifications and requirements to create a privacy information management system within an organization. Although its design and structure resemble closely ISO 27001, the two standards cover different subjects. While ISO 27001 relates to the way an organization keeps data accurate, available and accessible to approved employees only, ISO 27701 focuses on the way an organization collects personal and prevents unauthorized use or disclosure of personal data (International Standardization Organization, 2019). In other words, ISO 27701 is a privacy extension to the international information security management standard. In fact, like the standard for information security management systems, ISO 27701 adopts a risk-based so to allow organizations to identify specific risks to privacy and achieve compliance with applicable data protection regulation through the implementation of suitable measures.

2.2.6.4 Other relevant ISO standards

ISO/IEC 29190:2015 Information Technology - Security Techniques - Privacy Capability Assessment Model (ISO 29190)

ISO/IEC 29190:2015 presents the guidance on how to assess the capability of a given organization to manage processes related to privacy. The standard describes the different steps necessary to access the capability of an organization in the context of privacy. ISO 29190 specifies the different levels for the privacy capability assessment. At the same time, clear guidance is given in the standard on the main process areas to assess by the responsible members of the organization and finally, on the integration of the privacy capability assessment into the usual operations of the organization (International Standardization Organization, 2015a).

ISO/TR 12859:2009 Intelligent Transport System – System Architecture – Privacy Aspects in ITS Standards and Systems (ISO/TR 12869)

ISO/TR 12859 contains general guidelines "*to developers of intelligent transport systems (ITS) standards and systems on data privacy aspects and associated legislative requirements for the development and revision of ITS standards and systems*" (International Standardization Organization, 2009 para. 1.). In more detail, this report guides the development of the architecture and design of all ITS standards, systems and their implementation and serve as a roadmap to developers of ITS devices on general data privacy and protection aspects.

ITS involve extensive movement and exchange of data. Some data exchanged are anonymous, while others can reveal personal information. Nowadays, information cannot always be kept anonymous. Therefore, privacy is protected around the world by data privacy and data protection regulations. ISO/TR 12859 acknowledges that underlying principles of privacy and data protection are common across the globe, while each legislation adopts its own interpretation of those principles. In this sense, ISO/TR 12859 introduces a general framework to harmonize privacy and data protection approach in the development of ITS standards and systems. In fact, it is undisputable that ITS technologies will provide many opportunities to improve mobility and reduce its costs. On the other hand, designing ITS systems and standards shall give the highest consideration to legal and moral requirements for privacy and protection of data. This means taking into consideration the potential use and misuse of data in a system in order to achieve a desirable level of protection (International Standardization Organization, 2009). For this purpose, ISO/TR 12859 can be considered a valuable starting point to develop a common framework for privacy and data protection in ITS systems among members of the 5G-DRIVE project's consortium.

ISO 24100:2010 Intelligent Transport Systems – Basic Principles for Personal Data Protection in

Probe Vehicle Information Services (ISO/TR 24100)

This standard addresses the requirements for designing probe vehicle systems in compliance with data protection rules and policies. In general, it is expected that probe data collection systems will use suitable technical measures to minimize the collection of personal data and protect their use. However, if it is not possible to foresee in advance any possible threat, this report aims to provide clarifications on the best approach to ensure that probe vehicle systems are designed and deployed in accordance with data protection regulations. This standard is necessary because these systems collect and can reveal a great amount of sensitive personal information. This protection is particularly important because it is difficult to completely eliminate any possibility of probe data being linked to a specific individual or vehicle (International Standardization Organization, 2010).

The main objective of ISO/TR 24100 is the promotion of safe deployment and sound expansion of probe vehicle information services. This standard addresses the following issues:

"*a) If the providers of probe vehicle information services are not consistent in their handling of the privacy aspect of personal data, it could give rise to confusion in the marketplace and generate public mistrust of the services themselves. The development of this International Standard will facilitate the development of standard procedures common to all probe vehicle information service providers.*

b) Increasing the transparency of probe vehicle information services will enable drivers to know better in advance how probe data are to be collected and used, which will help dispel their anxieties about the possible misuse of their personal data.

c) Having an International Standard will allow more efficient research and development work on probe vehicle information systems and enhance the universality, commonality and interoperability of these services, thereby facilitating their smooth expansion" (International Standardization Organization, 2010, Introduction).

ISO 16461:2018 Intelligent Transport System – Criteria for Privacy and Integrity protection in probe vehicle information (ISO 16461)

ISO 16461 provides basic rules on probe vehicle information services. This is intended to be a tool for service providers to achieve compliance with their obligations and respect the privacy of their users. This document focuses on probe vehicle systems intended as systems collecting probe data from private vehicles for processing to produce useful information that can be provided to various end-users. In the context of ISO standards, this document is a further specification of ISO 24100. In particular, it clarifies the rights and interests of probe data subjects and aims at ensuring the protection of their privacy. This standard acknowledges that probe vehicle systems are subject to data protection regulations and, therefore, it intends to suggest protective measures and policies for implementation in these devices. The objective of this standard is to create a general framework for protecting the integrity of personal data and privacy of information gathered by probe vehicle systems. For this purpose, it identifies possible solutions for the protection of anonymity and integrity of probe data (International Standardization Organization, 2018).

With this aim in mind, ISO 16461 covers the: definition of security and privacy requirements for probe vehicle systems (PVS); specification of a common interface ensuring privacy and integrity in probe vehicle information acquisition; definition of a scheme for protecting probe vehicle systems in terms of integrity and privacy. In addition, the scope of this document also includes: the architecture of the PVS in support of appropriate protection of data integrity and anonymity in the PVS; security criteria and requirements for the PVS, specifically requirements for data integrity protection and privacy; requirements for correct and anonymous generation and handling of probe data (International Standardization Organization, 2018).

ISO/TR 17427-7:2015 Intelligent Transport Systems – Cooperative ITS – Part 7: Privacy Aspects (ISO/TR 17427-7)

ISO/TR 17427-7 is a document issued by ISO to increase awareness on possible privacy issues arising from the development, deployment and implementation of Cooperative Intelligent Transport System

(C-ITS). From this point of view, this report does not provide specifications for solutions to these issues. In general, C-ITS consists of multiple ITS technologies which communicate and cooperate to gather and produce enhanced information than those they would create absent communication and cooperation. These systems "*allow vehicles to 'talk' to each other [or] to the infrastructure [and] have significant potential to improve the transport network*" (International Standardization Organization, 2015b, Introduction)**.**

C-ITS are capable of presenting threats to privacy. In order to avoid these risks, it is necessary that C-ITS are subjected to control and regulations to prevent any abuse. In this sense, the document describes C-ITS devices and highlights privacy issues related to them. Through this identification process, the standard then suggests solutions to control and mitigate them, as well as ways to limit liability due to privacy violations (International Standardization Organization, 2015b).

2.2.6.5 Relevant ETSI standards

The European Telecommunication Standards Institute (ETSI) is an organization dedicated to the development of standards for the telecommunication industry. In the context of ITS, this institution has produced several guidelines for standardization purposes (*ETSI - Standards, Mission, Vision, Direct Member Participation*, n.d.).

ETSI TS 102 940 v1.3.1 (2018-04) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management (ETSI 102 940)

The ETSI 102 940 report provides identification of the functional entities necessary to support security in an ITS environment. To this end, the purpose and location of several security services are identified concerning the protection of transferred information and the management of the parameters necessary for security. The standard takes a holistic approach. It focuses on ITS architectures and possible security issues affecting them. Then the report highlights each of their threats that might jeopardize security, privacy and confidentiality. Using this approach, the standard guides several safety aspects in ITS, such as security requirements for ITS application groups, static local hazard warnings and advertised services. Lastly, it also provides a detailed overview of ITS communications security architecture (European Telecommunications Standards Institute, 2018).

ETSI TS 102 941 v1.3.1 (2019-02) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management (ETSI 102 941)

This ETSI standard aims to provide specifications to manage efficiently trust and privacy issues in ITS. According to the report, ETSI 102 941 "*identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS architecture*" (European Telecommunications Standards Institute, 2019, para. 1). The standard recognizes that trust and privacy management require secure distribution and maintenance of trust relationships. This relationship can be achieved through specific security parameters that embed enrolment credentials which are provided by third-party credentials of proof of identity or other attributes, such as pseudonym certificates (European Telecommunications Standards Institute, 2019, para. 4).

ETSI 102 941 promotes four key attributes in relation to privacy: anonymity, pseudonymity, unlinkability, and unobservability. Among these four features, the standard highlights that the most suitable solutions to achieve appropriate privacy protection are pseudonymity and unlinkability of personal information. According to the standard, the management of trust and privacy must cover the whole ITS lifecycle. This includes addressing trust and privacy in different stages: initial ITS configuration during manufacture; enrolment; authorization; operation and maintenance; end of life. The standard also highlights public key infrastructure that is essential to secure effective protection of trust and privacy in ITS (European Telecommunications Standards Institute, 2019).

2.2.7 Standards and recommendations - summary matrix

Standards	Key points
IEEE 1609 Family of standards	• Guidance on secure transmission of messages in Wireless Access in Vehicular Environments. • Standardize not only the architecture but the set of services and interfaces enabling wireless communications in vehicular environments. • Includes: IEEE 1609.0-2019, IEEE 1609.2-2016, IEEE P1609.2.1, IEEE 1609.3-2020, IEEE 1509.4-2016, IEEE 1609.11-2010, IEEE 1609.12-2019
ITU-T SG 17 Recommendations	• Promotion and production of standardization recommendations on communication technology. • Identifies security threats to connected vehicles and include security guidelines on effective prevention of attacks • Includes: X.1371, X.1372, X.1373, X.1374, X.1375, X.1376
ISO/IEC 27000 (ISMS) family of standards	• Establishes an information security management system within an organization. • Provides a framework for organizations to manage the security of their assets, information, or intellectual property. • Requires monitoring the risks to information security in an organization and examining possible threats and vulnerabilities. • Includes: ISO/IEC 27000:2018, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2018, ISO/IEC 27701:2019
ISO/IEC 29190:2015	• Different steps necessary to access the capability of an organization in the context of privacy.
ISO/TR 12859:2009 Intelligent Transport System	• Development of the architecture and design of all ITS standards, systems and their implementation. • A roadmap to developers of ITS devices on general data privacy and protection aspects.
ISO 24100:2010	• Promotion of safe deployment and expansion of probe vehicle information services.
ISO 16461:2018	• It is a further specification of ISO 24100. • Integrity of personal data and privacy of information gathered by probe vehicle systems. • Possible solutions for the protection of anonymity and integrity of probe data.
ISO/TR 17427-7:2015	• Awareness on possible privacy issues arising from the development, deployment and implementation of Cooperative Intelligent Transport System (C-ITS). • No specifications for solutions of these issues.
ETSI TS 102 940 v1.3.1 (2018-04)	• Identification of the functional entities necessary to support security in an ITS environment using a holistic approach. • Purpose and location of several security services in relation to the protection of transferred information and the management of the

Standards	Key points
	parameters necessary to security.
ETSI TS 102 941 v1.3.1 (2019-02)	- Trust establishment and privacy management to support security in an ITS environment.

Table 5: Standards and recommendations summary matrix

3 Requirement identification and potential solutions

This section will identify key requirements and introduce a set of innovative mechanisms that could be of relevance when addressing the main issues identified in section 2 towards the development of the future 5G vehicular networks. The mechanisms will be organized in two broad types: technical and organizational based on the business area which is most likely to be involved when implementing them, however they are not exclusive categories given the necessary interaction between the two.

3.1 Requirement identification

This section will consider the diverse sources showcased in Sections 1 and 2 to synthetize the normative dispositions identified in the previous section and identify a set of high-level requirements[4] for the three main areas of relevance to the 5G-DRIVE project: Connected vehicle Personal Data Protection compliance, V2X Security, and 5G privacy and security to be addressed by 5G-DRIVE's technical and organizational solutions (of special relevance in Section 3.2 and 3.3 below).

3.1.1 Connected vehicle PDP compliance

3.1.1.1 Enable Privacy Safeguards by Default

The introduction of a requirement to enable safeguards by design and by default as a core principle of personal data protection is a defining characteristic of the GDPR and other recent data protection regulations and has been integrated into several of the examined normative sources and standards.

Article 25 of the GDPR requires that "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*"(Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016).

In the V2X context, the EDPB has noted that considering "*the volume and diversity of personal data produced by connected vehicles, (…) data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data.*" (EDPB, 2020)

3.1.1.2 Identification of data categories

Most of the legal sources identified agree on the existence of diverse categories of data, which are subject to different levels of normative protection. Both in the Chinese and European contexts,

[4] Each requirement will be complemented with the relevant guidance from the European Data Protection Board, whenever possible.

sensitive or special categories of personal data are recognized and granted additional protection[5], likewise, non-personal or anonymized data is not subject to protection and can be transferred as necessary.

In the case of V2X enabled vehicles, the EDPB has noted that "*Most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tire pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations*[6]"(EDPB, 2020, p. 12)

In order to collect sensitive data (and particularly geolocation data), the EDPB has required compliance with the following principles: "*Configuration of the frequency and detail of the data collection, Accurate information to the data subject on the collected data, Valid consent mechanisms, Collection and processing of sensitive data only as required by user-requested functionalities (disabled by default); User-information of ongoing collection; Possibility to disallow collection at any time; Definition of a limited storage period*" (EDPB, 2020, p. 12)

3.1.1.3 Protection of traffic data

Traffic data is defined by the ePrivacy Directive as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication*" (European Parliament, 2002, Art. 2(b)). In the context of a 5G enabled IoV deployment or a 5G V2X deployment, traffic data and metadata constitute personal data which can be used to identify the data subjects and, in some circumstances (when intertwined with other data sources, for example), reveal special categories of personal data.

The ePrivacy Directive explicitly limits the conditions in which traffic data may be processed, with the upcoming entry into force of the ePrivacy Regulation, it is highly likely that the protection granted to traffic data will be enhanced. For this reason, both connected vehicles and V2X entities alike should carefully prevent the disclosure of this information to non-authorized parties.

3.1.1.4 Protection of location data

In a similar manner as the preceding point, location data can easily contain or indicate special categories of personal data, and must, for this reason, be granted protection by V2X entities. On this point, the EDPB adds that "*When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that geolocation data are*

[5] "Given the scale and sensitivity of the personal data that can be generated via connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in the art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies" (EDPB, 2020, p. 17).

[6] This type of data has been deemed particularly sensitive by the EDPB, and for this reason the Guidelines recommend their local processing of data, prohibiting external processing of data revealing criminal offenses or other infractions. (EDPB, 2020, p. 13)

particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centers of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller shall be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing." (EDPB, 2020, p. 12)

3.1.1.5 Data management / Data subject right compliance

Both the GDPR, the Chinese standard GB/T 35273—2017 and standards like ISO 27701 recognize several rights to data subjects, including rights of access, rectification, opposition, and deletion of personal data. This requirement aims to fulfil these, with the consideration of some additional particularities:

a) The data subjects are to be informed as soon as possible after a breach to their personal data has taken place.

b) The system upon which rights of access are exercised must be available as soon as possible after facing a data breach to ensure that the data subject remains in control of their personal data.

c) All necessary measures should be incorporated to ensure that if the data subject requests the deletion of its data, any controllers or processors who possess copies of the information must be informed and asked to comply with the request.

This point is supported by the EDPB, which mentions that: "*Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object*" (EDPB, 2020, p. 19).

The EDPB notes as well that "*Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR*" (EDPB, 2020, p. 17). While these elements are implementable in the context of connected vehicles (particularly those containing an infotainment system where the information can be displayed), they are quite challenging to implement in the context of a distributed deployment of V2X entities, as the data subject will not be easily informed about the complete range of entities, devices, organizations and service providers that have effectively obtained or processed his/her personal data.

Finally, the EDPB has recommended the implementation of an in-vehicle profile management system capable of facilitating settings modifications "*in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system in a vehicle should centralize every data settings for each data processing, especially to facilitate the access, deletion and removal of personal data from vehicle systems at the request of the data subject*" (EDPB, 2020, p. 17).

3.1.1.6 Data Retention Compliance

The examined standards and legislation (both in the Chinese and European contexts) recognize the need to establish rational data retention periods for the storage of personal data. Furthermore, they all recognize that upon its expiration, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays. All entities, service providers and data controllers related to future V2X deployments should utilize reasonable or non-extensive data retention periods and integrate necessary technical measures to ensure thatunnecessary personal data are neither requested nor registered (principles of storage limitation and data minimization). Furthermore, technical methods should be implemented to ensure that data is effectively deleted, and the process followed should be transparent towards end-users.

On this point, the EDPB recommends that "*Drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, except if a specific legislation provides otherwise or if the data are essential to the critical functions of the vehicle. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes*" (EDPB, 2020, p. 19).

3.1.1.7 Anonymization and Pseudonymization

As previously specified, the dispositions of the Personal Data Protection regulations and standards examined do not apply to anonymized data as long as the controller is able to demonstrate that they are not able to identify the data subjects (non-identifiability)[7]. To this end, it is recommended that "*If data must leave the vehicle, consideration should be given to anonymize them before being transmitted. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Once a dataset is truly anonymized and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymization, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles*" (EDPB, 2020, p. 16)

Whenever anonymization is not possible, "*Other techniques such as pseudonymization[8] can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing (…) Pseudonymization, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of misuse. Pseudonymization is reversible, unlike anonymization, and is considered as personal data subject to the GDPR*" (EDPB, 2020, pp. 16–17).

There are many implications to be considered when applying these two requirements in the context of connected vehicles, the 5GAA has particularly clarified that both Conditional Anonymity (individual vehicles should be anonymous within a set of potential participants) and Unlinkability (no entity should be able to link the different pseudonyms of a specific vehicle with each other) are key technical means to be considered when implementing privacy by design in V2X (5GAA, 2020, p. 10). As such, beyond their application in technical solutions detailed in Section 3.4, a potential certification scheme extension should take these elements into account (Section 3.5).

3.1.1.8 Records of processing activities and disclosures

In order to ensure compliance with the security requirement of non-refutability and accountability, and to guarantee compliance with the relevant data protection dispositions, the EDPB recommends the generation and maintenance of history logs of "any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies." (EDPB, 2020, pp. 19–20). These logs should be protected by strong security

[7] De-identification is a *"General term for any process of removing the association between a set of identifying data and the data subject"*(International Organization for Standardization, 2008, p. 3).

[8] Pseudonymisation consists of replacing directly identifying personal data by a non-signifying pseudonym. This can be done by, for example, using a secret-key hash algorithm. (EDPB, 2020, pp. 16–17).

mechanisms (such as encryption, physical safeguards and redundancies) and, in the context of the future 5G vehicular networks envisioned by this project, should be generated not only by vehicles, but also by other stakeholders in the V2X chain of custody of personal information.

3.1.1.9 Data breach information

Based on the principles of transparency and accountability of the GDPR and most other data protection regulations, the V2X entities, organizations and service providers should keep track and inform data controllers of breaches to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, thus enabling data controllers to take breach mitigation measures, and if required by law, inform the competent Data Protection Authorities and concerned data subjects of the situation.

3.1.1.10 Encryption of personal data by default

All personal data should be encrypted whenever it is stored or transferred. A strong encryption mechanism[9] should be selected to fulfil this requirement, including the adoption of state-of-the-art encryption algorithms and encryption key management, renewal and protection (at a per-vehicle basis); device authentication, integrity verification (e.g., by hashing) and usage of reliable user authentication techniques.

3.1.1.11 Update and review of privacy measures

According to this requirement, stakeholders involved in future 5G enabled vehicular networks should introduce technical and organizational measures guaranteeing that all V2X entities update and review their privacy measures, policies and mechanisms to ensure their effectiveness. This requirement is closely associated with the need to generate records of processing activities, data breaches and other events to enable their audit and cross-verification.

3.1.1.12 Security of processing (prevention of unauthorized access, alteration, disclosure and destruction of personal data)

In the context of 5G-DRIVE, Deliverable 4.3 identified the following list of security requirements for V2X communications: Authenticity, Integrity, Availability, Confidentiality, Access Control, and Privacy. These items will be further detailed in the following subsection. When addressing these topics, however, it is necessary to remember that security and personal data protection are intrinsically connected and while they have different specific objectives, their coordination is fundamental for the achievement of a reduced level of risk for both the organizations and the data subjects.

In the context of connected vehicles, the EDPB has provided some security recommendations that should be adopted by vehicle manufacturers. The EDPB recommends implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle; as well as "*partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment"); for the vehicle's vital functions, give priority as much as possible to using secure frequencies that are specifically dedicated to transportation; and setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode*" (EDPB, 2020, pp. 19–20).

In addition to this, the 5GAA has particularly noted that Minimum disclosure (the minimization of information disclosed to a user to that which is required for the normal operation of a system);

[9] Cryptographic protocols: TLS, IPsec, Kerberos, PPP with ECP, ZRTP, etc.

access control (as part of conditional anonymity mentioned before, understood in the sense that whenever a vehicle deviates from system policies it's access rights and identification should be retrievable and/or revocable); and forward and backward privacy (the revocation or vulnerating of a credential should not affect the unlinkability and privacy of other messages signed by the same sender) are fundamental privacy requirements for a V2X communications system (5GAA, 2020, p. 10).

3.1.2 V2X Security

V2X communications should be protected against security attacks to ensure trust in received data in terms of data integrity and sender authenticity. In addition, given the high mobility of moving vehicles and intermittent connectivity, the wireless channel is vulnerable to radio jamming attacks and consequently, it is not considered reliable. In the following, we briefly outline the different security threats of V2X communications. ETSI has highlighted in its report on threat, vulnerability and risk analysis (ETSI, 2017) that the most critical attacks are the denial of transmission and reception of data, modification and deletion of transmitted information, masquerade of a station, and acquisition of personal information. Moreover, data integrity, sender authentication and authorization, replay protection, and availability are mandatory security features that should be guaranteed in all V2X use cases.

3.1.2.1 Identification, Authenticity, and Integrity (IAI)

Basic safety messages (BSMs) or other messages that vehicle exchange are related to information about vehicle speeds, directions, etc. BSMs are regularly broadcast, usually at a rate of 10 Hz. If a vehicle transmits false information, other vehicles receiving it may trigger actions, which may generate accidents and casualties. Since these messages are transmitted over the air and received by many, source and message authenticity mechanisms need to be enforced. Hence, there is the need to ensure identification, the authenticity of the vehicles and integrity of the transmitted messages (Marojevic, 2018). By identification and authenticity, we express the ability to enable authorized access to services or information and authorized provisioning of services. The integrity of messages means the information is accurate and can be trusted. The integrity can be ensured by creating a digital signature over the message payload and packet routing information (Alnasser et al., 2019).

3.1.2.2 Availability (A)

The availability of vehicular applications and services should not be prevented by malicious activities. Therefore, increasing the capacity of V2X wireless communications to overcome the physically limited and shared resources is crucial. Indeed, if the wireless channel is congested, the availability of needed information is drastically reduced (Marojevic, 2018).

3.1.2.3 Confidentiality and Privacy (C&P)

The confidentiality ensures that the intended receiver only knows the transmitted information. To this end, it is usually assumed that the message is encrypted with the public key of the transmitter, where it only can be decrypted by the private key of the intended receiver (Alnasser et al., 2019).

On the other hand, different attributes of the vehicle, such as position, actions, and trajectory, need to be confidential to mitigate tracking and traceability of the vehicle.

3.1.2.4 Non-Repudiation and Accountability (NR&A)

Non-repudiation aims to identify the identity of the node which has performed a specific action. It ensures the message transmission between entities via digital signatures and/or encryption (Alnasser et al., 2019). For instance, connected vehicles rely mostly on GPS or other global navigation satellite system (GNSS) as the synchronization source but can use RSUs, base stations, or other vehicles. If no external source exists, frequency and timing drifts will occur that add up over time. This situation can result in system malfunctioning and harmful interferences. Urgent actions should be taken to recognize the vehicle causing this high level of interferences.

The table below outlines the different security threats and their impacts on the key security requirements of V2X communications.

	Fake nConfide nodes	False information	Fake certificates	RF congestion	Jamming	RF replay	Malfunctioning vehicles
IAI	X	x	x				
A			x	X	x		
C&P	X					x	
NP&A							X

Table 6: C-V2X Security threats and their impact on the key security requirements

3.2 5G-DRIVE High-Level Data Protection Assessment

Based on the identified requirements, the following section will introduce a high-level assessment of the actions undertaken in the 5G-DRIVE project, focusing particularly on compliance with personal data protection requirements. This assessment examines both eMBB and V2X trials with the main goal of showcasing the overall project compliance with data minimization and privacy by design requirements.

The goal of this exercise is to identify any potential issues of relevance for the project which should be considered by any of the project partners in case the eventual exploitation of the project results is sought. Furthermore, it serves to inform the technical and organizational solutions proposed in Sections 3.4 and 3.5. The presented information aggregates the results of continuous due-diligence actions undertaken throughout the project by all project partners as mentioned in other project deliverables.

Required information:	**Overall Assessment**	**Topic relevance for trials**			
		5GIC	**Espoo**	**JRC**	**Orange**
1) Context:	Assessment performed as a result of continuous compliance actions undertaken for the 5G-DRIVE H2020 project.	✓	✓	✓	✓
a. Project’s objectives	The 5G-DRIVE project is part of the H2020 ICT-22-2018 Call (“EU China 5G Collaboration”). This call aims at performing a close collaboration between the EU and China to synchronise 5G technologies and spectrum issues before the final roll-out of 5G. The main scope is to conduct 5G trials addressing two specific scenarios: • Enhanced Mobile Broadband (eMBB) on the 3.5 GHz band, which is a priority band in the two regions for early introduction of very high data rate services • Internet of Vehicles (IoV) based on LTE-V2X using the 5.9 GHz band for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) services, as well as the 3.5 GHz band for Vehicle-to-Network (V2N) communications	✓ ⊗	✓ ✓	⊗ ✓	✓ ⊗

Required information:	Overall Assessment	Topic relevance for trials			
b. Types of processing involved	• Non-personal data processing: Research data & test data generated by trials. • Personal data processing: No personal data from public sources[10] (see below); all undertaken tests carried out using non-personal data and/or research datasets. (the eMBB trial at Surrey[11] carried out three Augmented Reality demonstration events that could be classified as the processing of personal data. These activities were not publicly available and involved only a limited number of participants from the research teams)	✓ ✓	✓ ⊗	✓ ⊗	✓ ⊗
2) Nature of the processing:	Non-personal data (See D3.3 and 4.4):	N/A	N/A	N/A	N/A
a. Collection	No personal data from public sources was collected by any of the trials (Vedia C-V2X pilot[12] identified potential for collection or aggregation of data, however no such action was carried out in the trial and further practical testing with commercial vehicles would be required to prevent unauthorized collection in eventual exploitation of the solution.)	✓	✓	⊗	⊗
b. Use:	No personal data from public sources was used by any of the trials (AR Demo used some personal data from the research team. Use was limited to call duration)	✓	⊗	⊗	⊗
c. Storage	No personal data from public sources was stored by any of the trials	⊗	⊗	⊗	⊗
d. Deletion of data	N/A: No personal datasets were maintained by any of the trials. (AR Demo call data was not stored)	N/A	N/A	N/A	N/A
e. Source of data	No personal data was obtained from public sources (AR Demo data: research team members)	✓	⊗	⊗	⊗
f. Use of processors	No personal data processors were used by any of the trials	⊗	⊗	⊗	⊗
3) Scope of the processing:	1. eMBB: Test and validate the use of eMBB in the 3.5 GHz band through the use of typical mobile broadband services as well as Virtual and Augmented Reality (VR, AR).	✓	✓	⊗	✓

[10] Editor's note: The statements "no personal data from public sources" and "no personal data sourced from the public" are used to convey that effectively no personal data was effectively collected, processed, or stored by any of the 5G-Drive project trials, as noted in the assessment, minor processing activities involving personal data did take place throughout the project, notably for the three AR demo calls. As showcased in the table, these exceptions did not involve personal data from data subjects not-related to the 5G-Drive project (as data subjects were project researchers and the project coordinator).

[11] See D3.3 Section 2.1.1

[12] See D4.4 Section 4.1.3.1.

Required information:	Overall Assessment	Topic relevance for trials			
	2. V2X: Optimisation of the band usage in multiple scenarios with different coverages & validation of the geographic interoperability of the 3.5 and 5.9 GHz bands for these use cases.	⊗	✓	✓	⊗
a. Nature of the data	Non-personal data (AR Demo calls briefly used the image and voice of demo participants, obtained through a Microsoft Kinect 3d camera)	✓	⊗	⊗	⊗
b. Use of special categories of personal data	No special categories of personal data were used by any of the trials	⊗	⊗	⊗	⊗
c. Amount of personal data processed	No personal data from non-researcher data subjects were processed by any of the trials. (A small amount of personal data processing was involved as part of the AR demos)	✓	⊗	⊗	⊗
d. Frequency of data processing	Not Applicable, no personal data was used by any of the trials (AR Demo: data processing was not repetitive)	N/A	N/A	N/A	N/A
e. Retention period	Not Applicable, no personal data was used by any of the trials (no data was stored in the AR Demos)	N/A	N/A	N/A	N/A
f. Number of affected individuals	None (AR Demo: two researchers and project coordinator)	✓	⊗	⊗	⊗
g. Covered geographical area	Relevant jurisdictions: Personal Data usage: Geographic area of test does not reflect geographic-based personal data collection or processing activities	U.K. ⊗	Finland ⊗	Italy ⊗	Poland ⊗
4) Context of the processing:	5G-Drive H2020 Project	N/A	N/A	N/A	N/A
a. Relationship with the individuals	Not Applicable, no personal data from public sources was used by any of the trials	N/A	N/A	N/A	N/A
b. Data subject control over data	Not Applicable, no personal data from public sources was used by any of the trials	N/A	N/A	N/A	N/A
c. Inclusion of data from children or vulnerable groups	Not Applicable, no personal data from public sources was used by any of the trials	N/A	N/A	N/A	N/A
d. Existence of prior concerns over this type of personal data processing or	Not Applicable, no personal data from public sources was used by any of the trials.	N/A	N/A	N/A	N/A

Required information:	Overall Assessment	Topic relevance for trials			
security flaws					
e. Novel personal data processing activities	While the research performed as part of 5G-DRIVE involves intrinsically novel processing activities, this item is not Applicable, as no personal data from public sources was used by any of the trials.	N/A	N/A	N/A	N/A
5) Purposes of the processing:	No personal data processing activities were undertaken as part of the 5G-DRIVE project trials.				
a. Goals	1. eMBB activities focused on the Performance measurement and analysis of radio access technologies, 5g network technologies and Ensuring the interoperability between Chinese and European eMBB technologies. 2. V2X activities focused on the demonstration of 5G-based IoV scenarios; ensuring the interoperability between Chinese and European IoV technologies; testing 5G network capabilities to deliver Ultra Reliable Low Latency Communication (URLLC) for self-driving scenarios; validating 5G KPIs in terms of bandwidth, latency and communication ranges in different scenarios and pilot sites; and Evaluating V2V and V2N communications resilience against cyber/RF attacks and interference under real-life conditions.	N/A	N/A	N/A	N/A
b. Intended effect on individuals	None, no personal data from non-project related data subjects was used by any of the trials	⊗	⊗	⊗	⊗
c. Expected benefits of the personal data processing for data subjects	None, no personal data from non-project related data subjects was used by any of the trials	⊗	⊗	⊗	⊗
6) Consultation process:	Not applicable, no data subject information processed given research focus.	N/A	N/A	N/A	N/A
a. Consultation of individual's views[13]	Consultation not required given lack of personal data processing.	⊗	⊗	⊗	⊗
7) Assessment of necessity and proportionality:	Not necessary, no personal data sourced from the public was used by any of the trials	N/A	N/A	N/A	N/A
a. Lawful basis for processing	No lawful basis necessary for processing non-personal data in a research project. (AR Demo: Lawful basis: Consent)	✓	N/A	N/A	N/A

[13] Article 35(9) of the GDPR and relevant EDPB guidelines recommend the performance of consultation processes whenever carrying out high-risk personal data processing activities in order to obtain the views of affected data subjects.

Required information:	Overall Assessment	Topic relevance for trials			
b. Data quality and data minimization measures	Despite overall lack of personal data processing activities, data quality and data minimization measures were introduced by all trials to prevent capturing or use of personal data.	✓	✓	✓	✓
c. Data subject information	Not applicable, no personal data sourced from the public was used by any of the trials.	N/A	N/A	N/A	N/A
d. Data subject right support	Not applicable, no personal data sourced from the public was used by any of the trials	N/A	N/A	N/A	N/A
e. Use of processors	Not necessary due to lack of personal data processing by trials and lack of personal data processors	⊗	⊗	⊗	⊗
f. International data transfers	While none of the project trials performs any personal data processing activities as part of their core activities, the eMBB trial at Surrey carried out three AR-based demonstration events that could be classified as international transfers of personal data. Further details can be found below: During the joint kick-off meeting with China Mobile in November 2018, a first joint Augmented Reality (AR) demo was setup between China Mobile in Beijing, China and University of Surrey in Surrey, UK. During November and December 2019, the second joint AR demo was tested again between Surrey site and China Mobile site, several times. However, due to the updated network firewall security issues in China, the network performance (i.e., data rate and E2E latency) could not meet the requirements that were expected for this type of service. To overcome this practical situation, another joint AR demo was then set up between the Surrey trial site and Espoo trial site in December 2019. EU partners from the 5G DRIVE project and partners from the Chinese twin project participated in this demo at the Surrey site. Realtime video was captured through a Kinect sensor. The video was then transmitted through the 5G core network of Surrey trial network to the VTT trial site.	✓	✓	⊗	⊗

Table 7: 5G-DRIVE high level data protection assessment

3.3 Contextual overview of key issues

The previous sections provided a detailed overview of the most relevant legislative and standardization frameworks which have been considered throughout the research performed in 5G-DRIVE and which have inspired the range of possible solutions examined to tackle security and personal data protection risks. However, numerous issues still surround 5G connected vehicles: from (cyber)attacks that threaten not only the driver's (and their passengers') safety but others on the road; to additional concerns related to the privacy and security of the drivers as data subjects. As previously noted, governments, institutions, and organizations (both regional and global), have analyzed the potential and innovation capacity of 5G vehicular networks towards a safer, cleaner, and more efficient digital transformation. A common denominator in their state-of-the-art research points out the importance and relevance of focusing on issues such as cybersecurity, liability, or privacy to maximize their viability.

For instance, the European Commission, by recognizing the innovative capacity of 5G connectivity, not only develops policies, legislation, and standards at the European level but supports actions beyond (*Connected and Automated Mobility | Shaping Europe's Digital Future*, 2021). Such actions include the designation of 5G cross-border corridors (*5G Cross Border Corridors | Shaping Europe's Digital Future*, 2021), the setup of 5G trials involving over 1000km of highway system (*Connected and Automated Mobility: Three 5G Corridor Trial Projects to Be Launched at ICT 2018 Event | Shaping Europe's Digital Future*, 2018), the harmonization of C-ITS activities across Europe (*About: C-Roads*, n.d.), or the launching of the GEAR 2030 High Level Group for ensuring coherent policies within the EU (European Commission, 2016). Additionally, as 5G network security is crucial for the European Digital Single Market, the European Commission also endorsed a toolbox (*Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures | Shaping Europe's Digital Future*, 2020) of mitigating measures for addressing security risks related to the rollout of 5G networks. This toolbox will enable the strengthening of security requirements while systematically assessing risk profiles and applying relevant restrictions (*Commission Endorses EU Toolbox to Secure 5G Networks*, 2020).

ENISA, the European Union Agency for Cybersecurity, also took the initiative in guiding stakeholders in the domain of the connected vehicle by analyzing the number of cybersecurity threats faced by such systems. Previously, it has already investigated the issue of smart cars (European Union Agency for Cybersecurity, 2019) and automated driving (European Union Agency for Cybersecurity, 2021b), producing synthetic reports for enhancing user experience while maintaining safety. Following the issue regarding the application of UNECE Regulations and the sometimes-limited scope of ISO standards, ENISA developed a report titled "*Recommendations for the security of CAM*", aiming to identify gaps that existing standards fail to cover while providing solutions for cybersecurity-related challenges of connected and automated vehicles (European Union Agency for Cybersecurity, 2021a).

The EDPB also published a Guideline on connected vehicles for facilitating the compliance of processing of personal data. Here, the Board pointed out how the application of IoT in vehicular networks is especially sensitive in its context as it affects not only road safety, but its intrusive nature put strains on the possibility of full anonymization. The Guideline stresses the importance of stakeholder awareness for implementing appropriate safeguards that prevent the misuse of data. Furthermore, the Guideline provides general recommendations for stakeholders for using and establishing vehicular networks in the context of personal data protection, distinguishing the categories of data and their purpose (European Data Protection Board, 2021).

Many organizations view standardization activities as key to identifying threats and effectively tackling them beyond jurisdictions. To support their standardization activities, ETSI has designated an Intelligent Transport System committee (TC ITS) for addressing topics such as communication architecture, management, access layer protocols, etc. (ETSI, 2013a). Additionally, ISO is currently working on its next standard, ISO/SAE FDIS 21434, on cybersecurity-by-design approach for the initial phases of designing vehicles (International Standardization Organization, n.d.-b). Moreover, ISO/CD 24089 is also in progress that aims to regulate software updates in vehicles (International Standardization Organization, n.d.-a).

Apart from specific standards and related activities, these organizations often see added value in public discussions through conferences. For example, the IEEE recognizing their game-changing potential held their 8th conference on connected vehicles in 2019 and has been preparing for the next one to be held soon. The Conference promotes interaction between academia and the industry (IEEE, n.d.). IEEE has been also sharing a number of researches to further raise awareness in the topic, focusing on identifying the type of threats (IEEE Innovation at Work, 2020; IEEE Spectrum, 2020). Since 2005, the Symposium on the Future Networked Cars of the ITU has been bringing together experts of the industry to discuss the future of connected vehicles and the future of automated driving while strengthening public trust. The ITU does so by influencing key stakeholders of the industry from the technological and business point of view (*Automated Driving in Focus at 2021 Symposium on the Future Networked Car*, 2021; *How Automated Driving Can Pave the Way for Safe Mobility*, 2021; *Setting the Standards for Autonomous Driving*, 2021).

Other stakeholders have also analyzed the issues related to the use of 5G connected vehicles from the privacy perspective. In its latest report on connected vehicles, IBM stressed the role of cybersecurity as the users of smart cars become more aware of the risks related to their personal data. Addressing growing requirements from both legislative and data subjects' perspective requires stakeholders of the connected car ecosystem (e.g., manufactures, suppliers, retailers, etc.) to adopt a privacy-by-design and privacy-by-default approach (IBM, 2019). The latest White Paper published by Booz Allen Hamilton on connected vehicles also provides a high-level overview of privacy issues. The White Paper identified six key privacy principles that are essential for safeguarding data subjects' rights, including (1) transparency; (2) choice; (3) respect for context; (4) data minimization, de-identification, and retention; (5) data security, integrity, and access; and (6) accountability. This report is again aimed towards stakeholders for implementing privacy protection measures (Booz Allen Hamilton, 2019). Privacy International, a London-based charity organization for the protection of privacy, warns about potential flaws in the designing of IoT devices which increases the chance of attacks. They paint a less idealistic picture when stating "*(…) we need to make clear that 5G might not be able to fulfill the promise for more connectivity*" (Privacy International, 2019).

Considering this complex context, some of the solutions identified in this deliverable (particularly those found in Section 3.4) will address the intrinsic difficulties found in meeting the connectivity and efficiency goals of V2X and 5G technologies while complying with privacy by design principles, minimizing the disclosure of data and ensuring unlinkability and trust through advanced pseudonymization mechanisms. This being said, given the wide range of identified issues, requirements, and relevant frameworks involved, any such technical solutions should be complimented with solutions that may address end-user trust-generation and compliance validation from an organizational perspective.

One such issue of particular relevance to 5G-DRIVE relates to the identified divide between the requirements found in European and Chinese legislative frameworks, as well as the standards, recommendations and reports produced by institutions and organizations within and beyond the EU, it is clear that there is a strong focus on the identification, regulation and elimination of (cyber)threats. One of the main concerns is related to privacy and the protection of personal data but there is yet to be an efficient and harmonized solution on not only how to implement best practices but how to identify them. Regulations or standards focus on segments of the issue and there is no one-stop-shop policy framework surrounding these that is fully applicable. As such, in the context of 5G-DRIVE, there is an apparent gap between the European and Chinese approaches towards personal data protection and privacy that cannot be simply solved through the application of either Regulation or other standards. For example, at the moment, a car manufacturer based in China cannot prove that they can comply with every national jurisdiction and specific requirements (e.g., trans-border data flows, data localization requirements, etc.) without pursuing a costly legal process in every jurisdiction it seeks to enter. This poses a challenge to the application of innovative technologies in a global environment.

A potential solution can be found in the form of voluntary certification mechanisms, which are increasingly relevant in both European and Chinese contexts (as showcased in Section 2.2) and which have increasingly focused on homogenizing previously unaddressed areas such as personal data protection.

The GDPR mentions the term "certification" over 70 times (although it does not define it). Trustable certification solutions bridge the legal divides within existing jurisdictions while some even take into account other solutions, such as domain-specific requirements or standards (e.g., ISO or ITU-T). Therefore, they are key to the massification of 5G connected vehicles of 5G-DRIVE. The GDPR introduces certification mechanisms under Article 42 and 43 as a solution for data controllers to demonstrate their compliance. The voluntary certification system of the GDPR allows national supervisory authorities or accredited certification bodies to issue certifications based on demonstrated compliance independently from other existing certifications. It is important to note, however, that a certification does not reduce the responsibility of a data controller or a data processor to comply with the GDPR (Publications Office of the European Union, 2019). It is the task of the EDPB to define common criteria applicable across the EU that may lead to a definition of the European Data Protection Seal. Since the GDPR came into force, the EDPB published a Guideline for identifying certification criteria in accordance with Article 42 and 43 that was approved in 2019. The Guideline defines the role of Supervisory Authorities and Certification Bodies, as well as details the development and approval procedure for certification criteria, including the criteria for the European Data Protection Seal (European Data Protection Board, 2019).

Finding a certification scheme that is able to assess the compliance of diverse data processing activities effectively can be challenging. In this sense, we can argue that there are two main types of GDPR certification schemes, but not without disadvantages. Universal certification schemes are cost-efficient; especially if we consider their accessibility to small to medium-sized enterprises (SMEs), which is one of the main objectives stated in the GDPR (Publications Office of the European Union, 2019). Nevertheless, the main disadvantage of these schemes is that they are inherently limited in nature and do not allow the assessment of specific risks related to technology, for example. On the other hand, specialized certification schemes are able to certify specific categories of data processing, but this advantage makes them near-inaccessible and expensive to most businesses. Neither of the certification scheme solutions mentioned above is applicable to the complexity of data processing in connected vehicles, especially in the context of the 5G-DRIVE project, where we aim for building a bridge between the European and Chinese frameworks. Cost is an important factor in both certification solutions, as a GDPR certificate is valid only for three years and must be renewed based on the continuous demonstration of compliance. Therefore, consideration must be given to “hybrid” certification mechanisms that combine the advantages of universal certification schemes and their comprehensive lists of criteria together with the complementary national-, domain- and technology-specific criteria, making hybrid certifications the most effective in terms of not only compliance but cost considerations.

Currently, the only GDPR certification under the review of EDPB to be endorsed as a European Data Protection Seal is Europrivacy™/®. The Europrivacy Certification Scheme complies with all the necessary criteria (e.g., in terms of applicability and scope) identified by the 5G-DRIVE project and may very well be implemented successfully across jurisdictional borders to ensure vehicle and service providers overcome the identified difficulties associated with diverging protection standards granted by national and regional legal frameworks. Section 3.5.1 will further detail the benefits of the Certification Scheme as a solution that integrates both the technical and organizational approaches due to its focus on certification of individual data processing activities.

3.3.1 Contextual overview of Privacy and Security issues related to Network Slicing

Network slicing is defined in the context of 5G as a key feature allowing a clear separation of the resources into virtual networks. A slice is a virtual network having specific characteristics complying with requirements given for a specific use case. For example, a slice used for the transmissions of videos requires a large bandwidth and weak reliability. On the other hand, a slice used for IoT communications may have different requirements such as smaller bandwidth, increased reliability, very low latency, and increased coverage. This means that every slice generated using 5G network slicing for each use-case may have different properties.

The usage of 5G network slicing implies the installation and the deployment of new components inside the 5G infrastructure. As consequences, new risks concerning data protection appear. This section will highlight these risks.

3.3.1.1 Securing the IP layer

As the 5G telecommunication network is built with all the components connected to each other on an IP architecture, the components are exposing their interfaces on the IP layer, including the Web-interfaces. So, the attack surface is becoming bigger and the possibilities to hack one or several components are naturally increased. At the same time, the distributed nature of the network slicing and the dependencies on cloud elements are also increasing the attack surface for the hackers. This issue can also happen at the third-party level. Indeed, the developers of a third party building a new service or application related to 5G can eventually access the data on the 5G network, including the slices containing personal data, if the telecommunication operators open their 5G network slicing system to a third party.

On the network slicing infrastructure, all the communications should be secured at the network layer as the first step; this involves the utilization of IPv6 and IPsec between all the interfaces of the different elements of the 5G network slicing system. Furthermore, interactions between sensitive nodes (vehicle/data server for example) should utilize IP sec tunnel mode. A second point to consider is the systematic usage of secured version of communication protocols like HTTPS between the interfaces at the application layer. This implies that the transport layer is composed of protocols providing the encryption mechanisms like TLS for HTTPS (HTTP over TLS). Of course, the access to the interfaces should be managed in a way to strictly limit the interactions between the components of the 5G network slicing to the authorized ones. This can be achieved by setting up and controlling all the access rights on the different layers of the OSI model. For example, on the network layer, the utilization of white lists will reduce the risks to be hacked by unauthorized virtual machines or other connected devices. On the application layer, the services offered by the different providers should implement user management to manage the access rights (authentication and authorization).

3.3.1.2 Data localization

In a classical server/client approach, there are two parties: the service provider running the server offering the service and the client consuming the service; in this case, data processing is performed server-side with the legal responsibility of the service provider, accordingly to the law where the service provider is located. Network slicing may then introduce new players (the network slicing service provider) which may act as data processors, carrying out data processing activities at the network slice infrastructure level. This introduces further complexity to the issues surrounding jurisdiction definition.

In this context, it is important to ensure regulatory compliance by identifying all the actors involved in a 5G network slicing deployment and determine for each of them where the data is stored and processed. In this manner, the legal problems about the jurisdiction can be anticipated and the possible cross-border data transfers can be also detected.

3.3.1.3 Trustable cross-border transfers

A consequence of the virtualization of the network through Software Defined Networking (SDN)or Network Function Virtualization (NFV) technologies is the augmentation of possible transborder data transfer. In fact, Internet has no border, and an unwanted transborder data transfer can happen if the network slicing service provider is located outside the country or the European Union. In this context, the laws to respect data protection can vary from a country to another one and, consequently, change the manner to store or process the data in a cloud environment. The same measures enounced in the previous item can be used to identify the probable transborder data transfer. It is essential to determine each data controller and data processor for each type of data encountered in the network slicing deployment.

3.3.1.4 Data ownership determination

The complexity brought by the SDN/NFV technologies is illustrated by the different kinds of components in the 5G infrastructure architecture. These components can be hosted in different locations in the different contexts defined in the global 5G architecture: cloud, edge. For instance, some components used for V2X communications can be hosted in the MEC (Multi-access Edge Computing) and others in the cloud. In each case, the storage and the processing of the data are done in function of the services provided to the end-user (who can be a driver of a connected car). Technically speaking, there are different types of data controllers or owners: the end-users/drivers, the mobile telecommunications operators, the network slicing/cloud services providers and the application providers. All the actors must comply to the regulations and laws applied in their country and as already mentioned earlier, some differences can be observed between countries with unwanted side effects on the data ownership.

The issue concerning the data ownership can be solved by the basic measures already mentioned above: the identification of all the involved actors and the data generated and consumed by each of the actors. This allows the correct determination of the borders for each actor and how the data will be shared among the services provided by the actors. From this starting point, the responsibilities and the legal compliance legislation to be used can be clearly defined and applied inside the 5G network slicing.

3.3.1.5 Infrastructure control

An important shift in the 5G paradigm compared to older telecommunication technologies is the fact that the telecommunication operators are giving a part of their control to new network slicing service providers. This means that the telecommunication operators have fewer responsibilities as they are are delegated to the network slicing/cloud service providers. So, some network management operations are now made on the network slicing or cloud service providers who can be less experimented or serious than the traditional and experimented telecommunication operators and the level of security could be decreased, augmenting the risks for the data protection in the 5G infrastructure. Network slicing may then become shared environments where the responsibilities to ensure data protection are diluted among the different service providers and other eventual actors (e.g. a German car within a slice operated by a German network may roam to a different operator whenever crossing borders, which may bring it outside of those jurisdictions directly covered by the GDPR’s territorial scope). As such, each additional actor could potentially be a weak point in the chain of data transmission in a network slice.

The loss of control is the most problematic for the telecommunication operators, as the quality of service (QoS) or other points mentioned in a service-level agreement (SLA) can be disturbed by an actor (typically a communication service provider or a network slicing service provider) who does not strictly follow the expectations defined in the SLA. The first step to mitigate the risks is to ensure that all the actors involved in the 5G network slicing deployment are legally bound to a common SLA which should define well all the parameters to consider during the interactions between the different actors. In the same manner, all the actors should obtain the same technical and organizational measures in their premises and infrastructure to be able to correctly handle all the aspects linked to the data protection. This can be achieved by the certification of each actor using the dedicated standards or specifications like ISO 27001 (information security management system) or ISO 27017 (cloud security). If all the actors are certified, a common technical and organizational basis will be present and will ensure that all the involved actors have sufficient knowledge to implement all the requirements and to solve all the issues associated with the data protection in the context of the 5G network slicing.

3.3.1.6 Security level standardization

As the actors working in the different parts of the 5G infrastructure are heterogeneous and have different business objectives at the end, the application of the security and privacy recommendations or good practices can be slightly different from an actor to another one. These differences could create weak points in the complete chain of data transmissions among the components of the 5G infrastructure. In this context, there are also possibilities that the different kinds of service providers, like network slicing, cloud, and communication service providers, are concurrent and the fiery competition between them could impeach a good collaboration to ensure good security in the 5G infrastructure. In this context, the different actors would probably not share their security and privacy management policies, making it harder to evaluate the real level of security of a 5G network slicing deployment.

The level of security depends mainly on two factors already enounced above: the localization of the actor (the telecommunication operator or the communication service provider) and the technical and organizational competences of the actor. Indeed, the localization of the actor implies by itself which laws or regulations the actor must follow. The level of competences of an actor can be determined through well-known certification and audit processes. This should ensure at the end a particularly good level of security among the different actors existing in the 5G network slicing deployment.

3.3.1.7 Data confidentiality assurance

The 5G network slicing is intended to create end-to-end (E2E) communications in the global mobile network. The data is transferred between several components and eventually, services that are managed by different actors implementing different regulations and good practices. If the chain of data exchange is not well done in accordance with the European standards in terms of data protection, the data confidentiality could be compromised, and data leakage will happen. To ensure the confidentiality of the data in transit between elements of the 5G network slicing infrastructure, data encryption should be mandatory in all the path used by the data. So, all the involved actors must comply to this rule for personal and sensitive data using the 5G network slicing services.

3.4 Technical solutions

3.4.1 Situation-centric and dynamic pseudonym changing strategy for SDN-based 5G Vehicular Networks

Location privacy is an important issue for future 5G vehicular networks. Indeed, the public acceptance of this technology can strongly be affected if the location privacy of users is not well protected. The standardized approach to ensure location privacy in vehicular networks is the frequent changing of pseudonyms. However, several studies have been demonstrated that this approach could not provide the required protection, without using an effective pseudonym changing strategy. Therefore, a synchronization of the pseudonyms changing schemes between vehicles is crucial to ensure a high level of location privacy protection. In this context, many pseudonym changing strategies have been proposed (Abdelwahab Boualouache et al., 2017). However, most of the proposed strategies are static, rigid and not adapted to the context i.e., once the security parameters of strategy are configured, they could not dynamically be changed according to the current situation or context of the vehicles.

To overcome this limit, we propose a new SDN-based pseudonym changing strategy. This strategy uses SDN controllers as the strategy coordinators and relies on them to change the security parameters of pseudonym changing strategy. This proposed strategy supports both infrastructure and infrastructure-less vehicular zones.

3.4.1.1 Vehicular System model and Assumptions

We consider vehicular networks in a heterogeneous environment that comprises vehicular zones equipped with the 5G infrastructure and infrastructure-less vehicular zones. We also assume that vehicles are periodically forming and updating vehicular clusters using a clustering algorithm. The clustering helps to reduce interfaces and overhead and to provide better support for density and mobility. In addition, as the cluster head (CH) will play the role of a local SDN controller, the used clustering algorithm should ensure the maximum stability of the cluster head, which will help to minimize the frequency of changing of the cluster head, and thereby the SDN controller.

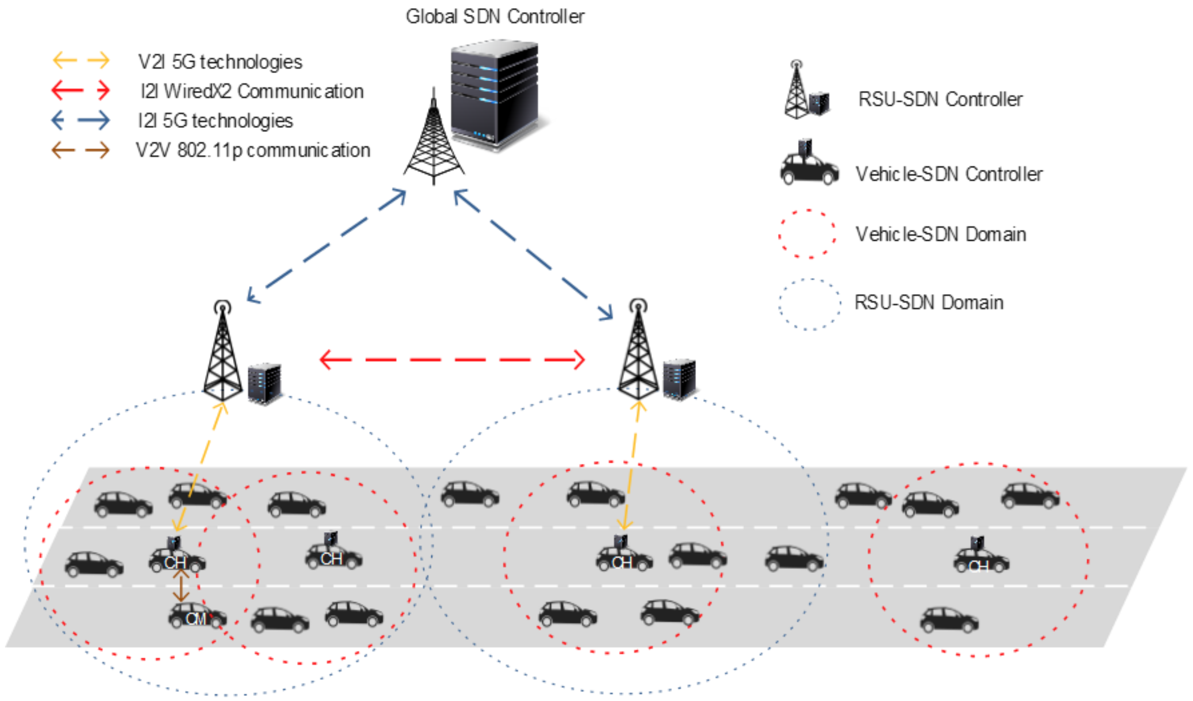


Figure 1: Reference Architecture

We also adopt a hierarchical architecture of multi SDN controllers similar to the one proposed in (Alioua et al., 2017). As illustrated in Figure 1, there are three SDN control levels in this architecture. The first one is a local SDN controller of each cluster SDN. As previously mentioned, we assume that each elected cluster head (CH) will play the role of an SDN controller within its cluster, and thereby the coordinator of the pseudonym changing strategy. This local SDN controller is called Vehicular-SDN Controller (VSDNC), and its cluster is called then the Vehicular-SDN controller domain. The second level of the control plane is the RSUs. Each RSU (eNodeB) holds an SDN controller and has its own control domain, which is larger than the first level of the control. The RSU-SDN Controller (RSDNC) can control several vehicular clusters according to the communication range of the RSU. Therefore, each RSU has a regional knowledge about its domain. Finally, the third level is the global SDN controller that has a global knowledge about the vehicular network. Besides these three levels of the SDN control plane, all the rest of the vehicles belong to the forwarding plane.

Each vehicle is equipped with two interfaces: 802.11p interface to communicate with other vehicles and a 5G interface to communicate with RSUs (eNodeBs). An SDN controller and an SDN agent are also running on each vehicle. While the SDN agent should be always activated, the SDN controller is initially deactivated, and it will only be activated when the vehicle turns to a cluster head and deactivated again if the vehicle turns to a cluster member (CM). The internal clocks of vehicles are synchronized using GPS signals, for instance.

Each RSU (eNodeB) is also equipped with two interfaces. A wired X2 link to connect with the neighbouring RSUs and a 5G interface to communicate with the global SDN controller. Each RSU is running an SDN controller. The global SDN controller is hosted in a distant location. The communication link between the local SDN controller (VSDNC) and the vehicles is secured. The communication links between the SDN controllers of the three level of control are secured as well.

Each vehicle periodically broadcasts a safety message every t millisecond, where each message includes the current location and the velocity of the vehicle, the timestamp, and the content that the vehicle is carrying. Before joining the vehicular network, each vehicle registers with the CA (certification authority). During registration, each vehicle Vi is pre-loaded with a set of m pseudonyms Ki,k where k ∈ {1,..., m }, that are, public keys certified by the CA. For each pseudonym Ki,k of a vehicle Vi , the CA provides a certificate Certi,k (Ki,k). The safety messages are properly signed by private keyK−1i,k corresponding to the pseudonym Ki,k to ensure the authentication. A certificate is attached to each message to enable other vehicles to verify the sender's authenticity.

Adversary model

We are interested in studying the location privacy protection against an external global passive adversary. This adversary aims to track the target vehicle by eavesdropping on all communications of any vehicle within a region of interest.

Description of the proposed strategy

In this section, we describe the proposed SDN-based pseudonym changing strategy. This strategy has three steps: (i) the installation of the security parameters of the pseudonym changing strategy (PCS), (ii) the local SDN monitoring and the pseudonym changing process, and finally (iii) the dynamic changing of the PCS security parameters and the update of the SDN controllers.

PCS security parameters installation

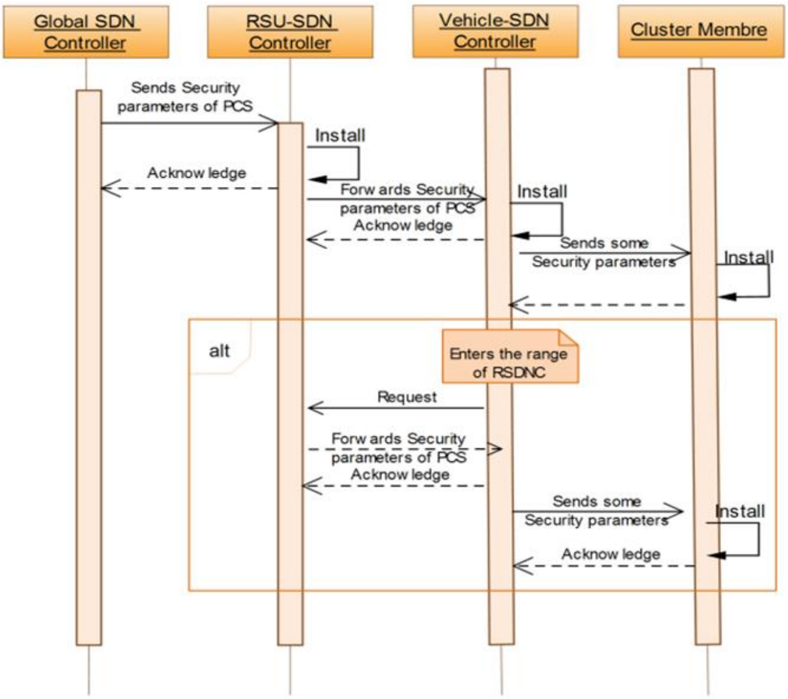

Global SDN Controller
RSU-SDN Controller
Vehicle-SDN Controller
Cluster Membre
Sends Security parameters of PCS
Install
Acknow ledge
Forw ards Security parameters of PCS
Install
Acknow ledge
Sends some Security parameters
Install
alt
Enters the range of RSDNC
Request
Forw ards Security parameters of PCS
Acknow ledge
Sends some Security parameters
Install
Acknow ledge

Figure 2: PCS security parameters installation

As shown the Figure 2, after the creation of vehicular clusters, the global SDN controller sends the security parameters of the Pseudonyms Changing Strategy (PCS) to RSDNCs. Each RSDNC will install these security parameters as soon it receives them. Then, it will send back an acknowledgement to the global SDN controller and forwards these security parameters to each controlled VSDNC. However, in the case of the infrastructure-less scenario, the VSDNC may be outside the range of the RSDNC. For this reason, we assume that a set of default PCS security parameters are already installed at the VSDNC. These parameters will be updated as soon as the VSDNC is in the range of a RSDNC. Each VSDNC will then install the PCS security parameters and send back an acknowledgement to RSDNC. Then, it sends necessary PCS security parameters to each cluster member and starts monitoring them. It is worth noting here that VSDNC can reach out an all the cluster members as it is the cluster head.

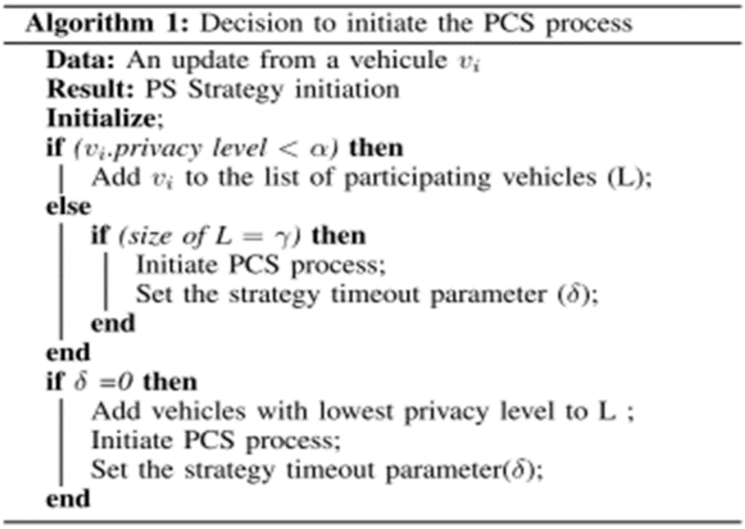
The following security parameters are considered by the pseudonym changing strategy:

- **The threshold of privacy (α):** is the threshold under which the vehicle should change its pseudonym

- **The frequency of changing of pseudonyms (β):** defines the number of pseudonyms that will be used each hour.
- **The number of required vehicles (γ):** defines the number of candidate vehicles required to initiate the pseudonym changing process.
- **The strategy timeout (δ):** defines the duration above which the pseudonym changing process should be initiated.

3.4.1.2 Monitoring and pseudonym changing

Each SDN-agent periodically sends an update to its local SDN controller (VSDNC). These updates generally include the mobility parameters (position, speed, and acceleration) of vehicles and their current privacy level. These updates are used by VSDNCs to select the vehicles that can participate in the next process of changing pseudonyms. A vehicle is selected to participate in the next round of pseudonyms changing operation if it only meets a specific context. The context is defined by the PCS security parameters that are forwarded by the global SDN controller. It mainly includes the threshold of privacy, the number of required vehicles, and the strategy timeout.



```
Algorithm 1: Decision to initiate the PCS process
  Data: An update from a vehicule $v_i$
  Result: PS Strategy initiation
  Initialize;
  if ($v_i$.privacy level $< \alpha$) then
      Add $v_i$ to the list of participating vehicles (L);
  else
      if (size of L $= \gamma$) then
          Initiate PCS process;
          Set the strategy timeout parameter ($\delta$);
      end
  end
  if $\delta$ =0 then
      Add vehicles with lowest privacy level to L ;
      Initiate PCS process;
      Set the strategy timeout parameter($\delta$);
  end
```

Figure 3: Decision to initiate the PCS process

As shown in Figure 3, a vehicle v_i is added to the list (L) of vehicles that will participate in the next process of changing pseudonyms; only its privacy level is below the privacy threshold parameter **(α)**. If the number of vehicles included in L equals the number of required vehicles **(γ)**, the pseudonyms changing process could be initiated. In addition, if the number of vehicles included in L is less than **γ** and the strategy timeout is expired, the VSDNC will fill the list L by the vehicles that they have the slowest privacy levels and initiate the pseudonyms changing process. The strategy timeout **(γ)** should also be initialized after the initiation of PCS process.

When the PCS process is initiated, VSDNC sends a command to all its cluster members to initiate a simultaneous change of their pseudonyms at a given time **(t)**. The whole PCS process is controlled by the VSDNC. The new privacy levels of vehicles participating in PCS process will be calculated by the VSDNC after the end of the process.

3.4.1.3 Security parameters update

The SDN controllers at the three levels of the SDN control plane exchange information between them in order to ensure an efficient and well-synchronized pseudonym changing strategy. Each VSDNC reports information to its regional domain controller (VRSUC) in order to keep track of the vehicles changing their clusters. In addition, the VSDNCs report the new created clusters information and the efficiency of the applied pseudonym changing strategy to the global SDN controller via RSDNCs. The purpose of this exchange is to tune the PCS security parameters according to the archived performances. The PCS security parameters can be tuned as follows:

The frequency of changing of pseudonyms (β): high frequency value has a positive impact on location privacy. However, a higher frequency of changing could have negative impacts on the applications performances and will increase the number of used pseudonyms, and thereby a huge storage space could be needed to store them. Subsequently, this frequency should be carefully tuned by the global SDN controller according to adversary power.

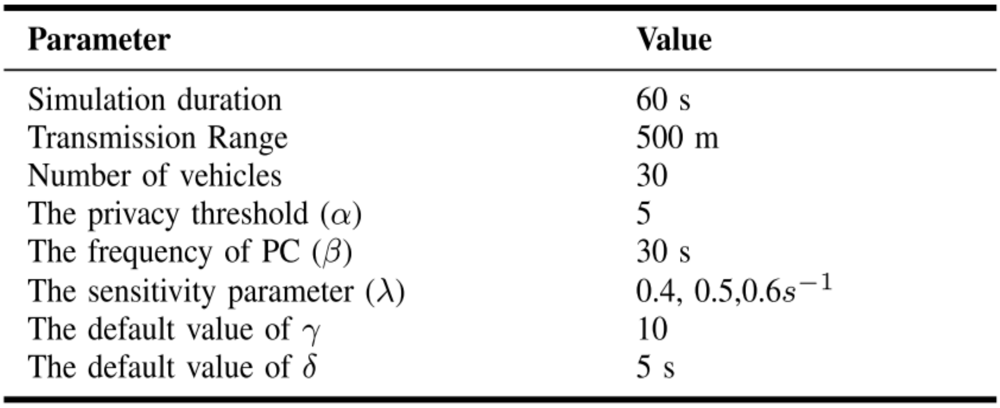
The threshold of privacy (α): this parameter could also be tuned by the global SDN controller according to preferred levels of privacy protection that are provided by users. For example, this parameter could regularly be calculated based on the average of the preferred levels of privacy protection.

The number of required vehicles (γ): a high number of vehicles change their pseudonym together has a positive impact on location privacy protection. However, as long as the decision to initiate a PCS process depends on obtaining a required number of vehicles, the PCS may not perform well if this parameter is not well tuned. Indeed, this parameter directly depends on the number of cluster members and which of them have a privacy level under the threshold of privacy. This parameter is thus indirectly depending on the vehicular density and there should of privacy parameter. The global SDN controller should thus be tuned this parameter according to the information received from VSDNCs.

The strategy timeout (δ): this parameter is closely related to the **γ** parameter. It helps to execute the pseudonyms changing strategy when the number of required vehicles is not achieved. This parameter should be tuned to prevent executing unnecessary PCS process.

3.4.1.4 Performance evaluation

We simulate our SDN-PCS scheme using Veins, an inter-vehicular communication simulation framework based on two well established simulators OMNet++ (C. Sommer et al. 2011) and SUMO (*Eclipse SUMO - Simulation of Urban MObility*, n.d.). Table 8 summarizes the parameters considered in our simulations.

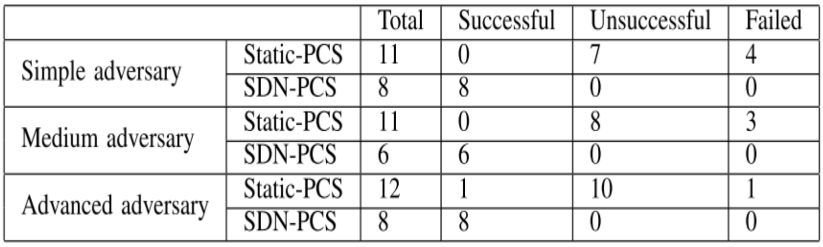


Parameter	Value
Simulation duration	60 s
Transmission Range	500 m
Number of vehicles	30
The privacy threshold (α)	5
The frequency of PC (β)	30 s
The sensitivity parameter (λ)	0.4, 0.5,0.6s^{-1}
The default value of γ	10
The default value of δ	5 s

Table 8: Simulation Parameters

We consider the case of a highway. We simulate a two-lane straight road section of 1.5 Km. We focus on the impact of the proposed strategy on a given cluster. The privacy level values of vehicles are initialized using a normal distribution N (μ,σ) with a mean equal to μ = 8 and with a standard deviation equals to σ = 5/3. In addition, as shown in Table 2, fixed values are used to initialize some of the security parameters such as the privacy threshold (α), the frequency of pseudonym changing (β). However, other security parameters such as the number of required vehicles (γ) and the strategy timeout (δ) are initialized with default values and updated within simulations. We compare our proposed strategy to a Static PCS: a typical PCS that sums up all the existing PCSs where security parameters are static such as mix-context (M. Gerlach and F. , 2007) and Rep (A. Wasef and X. Shen, 2010). We also consider three levels of adversary power: simple (λ= 0.4s $^{-1}$), medium (λ=0.5s $^{-1}$) and advanced (λ=0.6s $^{-1}$). Table 3 shows the number of the performed PCPs for each adversary level using the static PCS and the SDN-PCS. PCPs can be classified according to their results into three cases: (i) Successful: in this case, the PCP runs after an optimal timeout and the number of vehicles that have privacy level under the threshold of privacy is equal to γ; (ii) Unsuccessful: While the PCP is performed, the number of vehicles that have a privacy level under the threshold is higher than γ; these vehicles will not be included in the PCP if the security parameters are not adequately adjusted; and finally (iii) Failed: in this case, the PCP is not preformed because the number of required vehicles that are under the threshold is less than γ after the timeout. In total, the number of performed PCPs in the case of the static PCS is higher than the SDN-PCS.

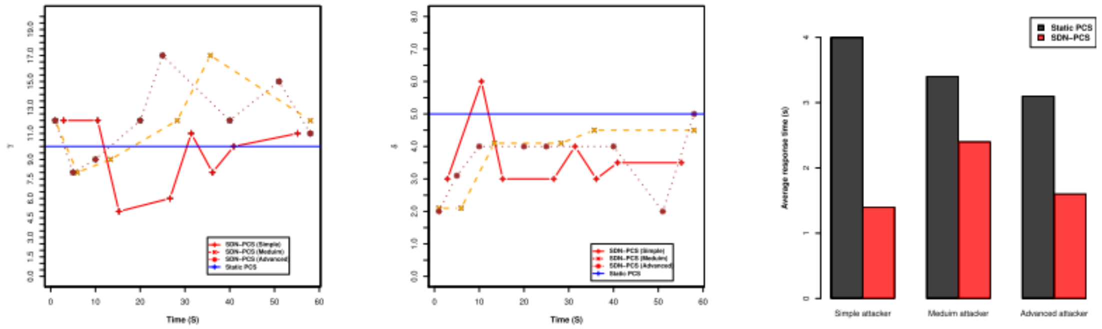
Our approach optimizes the number of PCPs to be executed i.e., the PCP is initiated only if necessary. The SDN-PCS achieves 100 % successful PCSs. Indeed, the SDN-PCS adjusts the security parameters dynamically according to the vehicle's context before each process. However, in the static PCS almost 0% of PCPs are successfully executed. The rest PCPs are either are unsuccessful (between 64% and 73%) or failed (between 8% and 36%). This is due to the fact that static PCS keep the security parameters unchanged, whatever the PCS process is.



		Total	Successful	Unsuccessful	Failed
Simple adversary	Static-PCS	11	0	7	4
	SDN-PCS	8	8	0	0
Medium adversary	Static-PCS	11	0	8	3
	SDN-PCS	6	6	0	0
Advanced adversary	Static-PCS	12	1	10	1
	SDN-PCS	8	8	0	0

Table 9: SDN-PCS vs static PCS: Statistics on the pre-formed PCP with different adversary power levels

Figure 4a and Figure 4b show respectively the variation of the number of required vehicles (γ) and the strategy timeout (δ) over time in function of the adversary power. In contrast to static-PCS, PCS-SDN automatically adjusts these security parameters before each PCP. For instance, SDN-PCS increases the number of required vehicles to perform the PCP when the adversary is powerful to increase his confusion. However, when the adversary is weaker, fewer vehicles are required to perform PCS and hence SDN-PCS decreases the strategy timeout to provide optimal response time. The strategy timeout results (Figure 4b) confirm the efficient tuning performed by SDN-PCS. Weaker is the adversary, longer is the PCP expiration time. Static-PCS keeps the same PCS parameters values despite the change of the vehicle context. These dynamic configurations of PCS security have positive impacts on the response time. This latter is defined by the delay between the triggering of the PCS and the time when the pseudonym is effectively changed. As illustrated in Figure 4c, the average of response time is improved by more than 38% when using SDN-PCS. In addition, we evaluate the evolution of the privacy levels of vehicles over time. To this end, we use the anonymity set size as the privacy metric. The anonymity set size is defined as the number of vehicles that have participated in the PCP (γ). The privacy level of a vehicle vi will then increase by (γ) each time it participates in the PCP. Figure 5 plots the overall privacy level, which is calculated based on the average of all privacy levels of vehicles over time. For both Static PCS and SDN-PCS, the average levels of privacy remain above the threshold. It is worth mentioning that the overall average of privacy levels of vehicles using SDN-PCS is higher than one provided by static PCS.

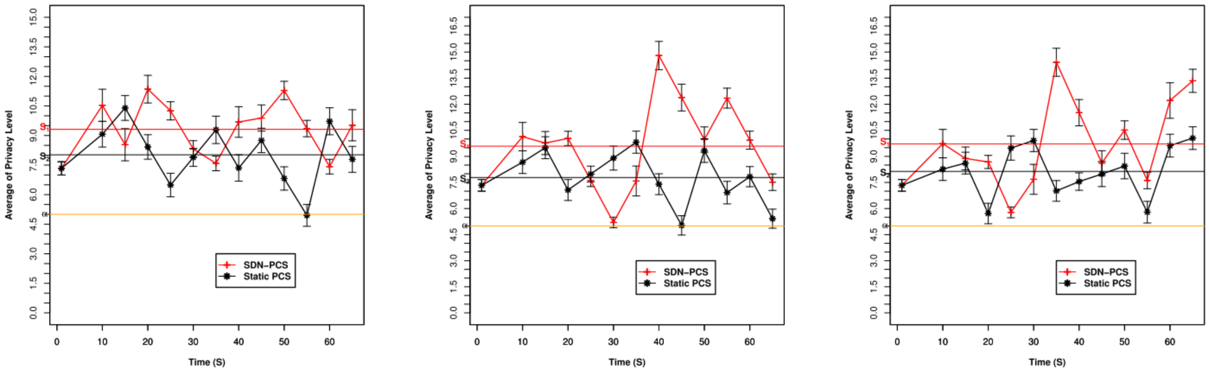


(a) The variation of of the number of required vehicles (γ).

(b) The variation of the strategy timeout (δ).

(c) Average of response time.

Figure 4: Security parameters update and response time



(a) Simple adversary.

(b) Medium adversary.

(c) Advanced adversary.

Figure 5: The average of privacy levels of vehicles over time

We evaluate in Table 10 the overhead in terms of the number of messages needed to accomplish the PCS using SDN-PCS and Static PCS. It is obvious that our approach causes less overhead. Indeed, more than 54% of messages are saved. The reason for this that SDN-PCS sends pseudonym changing requests only if needed.

	Static PCS	SDN-PCS
Simple adversary	200	91
Medium adversary	220	70
Advanced adversary	292	112

Table 10: PCS overhead: SDN-PCS vs static-PCS

3.4.2 Privacy-by-design approach for SDN-based 5G Vehicular Networks

Making personal data anonymous is crucial to ensure the adoption of connected vehicles. One of the privacy-sensitive information is location, which once revealed can be used by adversaries to track drivers during their journey. Vehicular Location Privacy Zones (VLPZs) is a promising approach to ensure unlikability. These logical zones can be easily deployed over Roadside infrastructures (RIs) such as gas station or electric charging stations. However, the placement optimization problem of VLPZs is NP-hard and thus, an efficient allocation of VLPZs to these RIs is needed to avoid their overload, and the degradation of the QoS provided within these RIs. This work considers the optimal placement of the VLPZs and proposes a genetic-based algorithm in a software-defined vehicular network to ensure minimized trajectory cost of involved vehicles and hence less consumption of their pseudonyms. The analytical evaluation shows that the proposed approach is cost-efficient and ensures a shorter response time.

3.4.2.1 Background

Vehicular Location Privacy Zone (VLPZ) is a logical zone that aims at protecting the location privacy of vehicular users. The internal design of VLPZ is seemingly similar to RIs such as gas stations and vehicle charging stations. Indeed, a basic VLPZ consists of one entry point called the router, one exit point called the aggregator and a limited number of lanes *l* where *l*>1. For this reason, VLPZs can easily be placed on RIs. In addition, VLPZs can be created as independent RIs in future vehicular networks given the urgent need of protecting the location privacy of road users. Figure 6 illustrates a two-way street where two VLPZs are installed: (i) VLPZ$_1$: for vehicles coming from West to East, and (2) VLPZ$_2$: for vehicles coming from East to West.

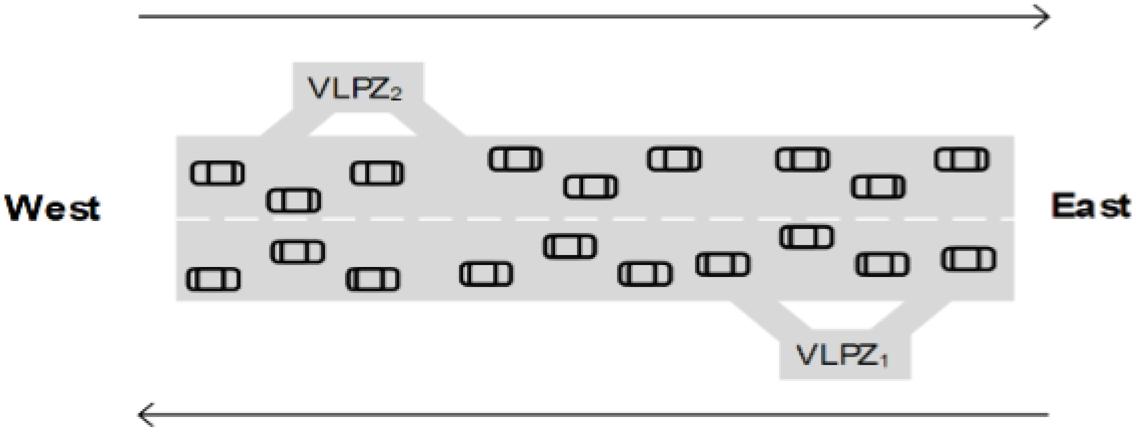


Figure 6: Multiple VLPZs models

Inside the VLPZ, vehicles can change their pseudonyms in a secure way as follows: vehicles arrive at a VLPZ, one after another, on a one-lane. When a vehicle reaches the router, it stops broadcasting safety messages and heads for an assigned VLPZ's lane. The assigned lane is randomly and privately selected by the router. The vehicle can then reside inside a VLPZ for a random period of time, depending on the service time. A vehicle must change its pseudonym before leaving the VLPZ and all vehicles exit a VLPZ through the aggregator. This strategy provides the protection not only against both of the syntactic and the semantic linking of pseudonyms but also against the FIFO attacks. In addition, unlike the strategies that rely on the radio silence technique, safety implications are limited in this strategy since the speed of vehicles inside VLPZs is very low, which ensures a good tradeoff between privacy and road safety.

3.4.2.2 System model and problem formulization

In this section, we present the proposed software-defined vehicular network architecture and give the formalization of the optimal placement of the VLPZs problem.

- **Vehicular system model**

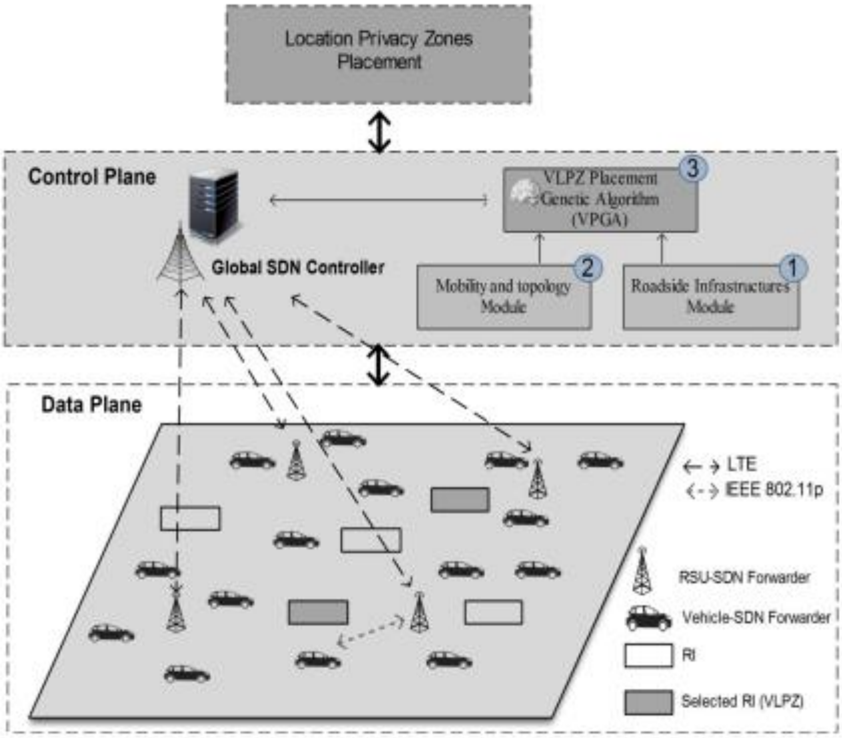

Location Privacy Zones Placement
Control Plane
Global SDN Controller
VLPZ Placement Genetic Algorithm (VPGA)
3
Mobility and topology Module
2
Roadside Infrastructures Module
1
Data Plane
LTE
IEEE 802.11p
RSU-SDN Forwarder
Vehicle-SDN Forwarder
RI
Selected RI (VLPZ)

Figure 7: Software-defined vehicular network architecture

We consider a software-defined vehicular network architecture. As illustrated in Figure 7, this architecture has one level of SDN control consisting of the global SDN controller that has full knowledge about the vehicular network. The data forwarding plane consists of vehicles and Road Side Units (RSUs). Each vehicle is equipped with 802.11p interface to communicate with other vehicles and with RSUs. Each RSU is also equipped with two interfaces. A wired link to communicate with the neighboring RSUs and an LTE interface to communicate with the global SDN controller. An SDN agent is also run on each vehicle and RSU. The communication links between the global SDN controller and the data plane are secured. We also consider that the road area contains a set of RIs managed by trusted authorities. RIs periodically send updates including their current capacity to the global SDN controller. The internal architecture of the global SDN controller mainly consists of three modules:

1) **Roadside Infrastructure Module (RIM):** it collects information and updates about the RIs.

2) **Mobility and Topology Module (MTM):** it collects the mobility information of vehicles.

3) **VLPZ Placement Genetic Algorithm (VPGA):** it selects periodically the best RIs to host the VLPZs based on the information provided by RIM and MTM. When a vehicle decides to enter a VLPZ, it sends a request to the global SDN controller. This latter uses the solution provided by the VPGA to assign each vehicle to the adequate VLPZ. Each vehicle periodically broadcasts a safety message every t millisecond, where each message includes a location, a time, a velocity and content. Before joining the vehicular network, each vehicle registers with the CA (certification authority).

During registration, each vehicle V_i is pre-loaded with a set of m pseudonyms $K_{i,k}$ where $k \in \{1,...,m\}$, that are, public keys certified by the CA. For each pseudonym $K_{i,k}$ of a vehicle V_i, the CA provides a certificate $Cert_{i,k}$ (K i,k). The safety messages are properly signed by private key $K^{-1}_{i,k}$ corresponding to the pseudonym $K_{i,k}$ to ensure the authentication. A certificate is attached to each message to enable other vehicles to verify the sender's authenticity.

- **Problem formalization**

Here we answer the following question: Given m RIs that exist in a road area, with m>= N_{max} , what are the best RIs that should deploy VLPZs in order to reduce the trajectory cost of vehicles ?

To answer to this question, we formulate the problem as follows: Let i= { 1,...,n} the set of existing vehicles at time t. Let j={1,...,m} be the set of the candidate RIs to deploy the required VLPZs. Let c ij the trajectory cost of a vehicle v_i to move to a RI $_j$. Let y j a binary decision variable, which indicates that the RI is selected to host a VLPZ at time t. x_{ij} is a binary variable, which indicates that the vehicle v_i is assigned to RI j or not. To select the best RIs that host the required number VLPZs, we should minimize the following objective function F, which aims to minimize the trajectory cost of vehicles when moving to the assigned VLPZ (Boualouache et al. on PRIVANET, 2019).

$$F = min \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} x_{ij} \quad ... (1)$$

Formula 1

The transportation cost c_{ij} can be expressed as the time spent by a vehicle v_i to reach a candidate RI_j and quantified by the loss of pseudonyms during this time, which can be calculated using the following formula:

$$cij = \frac{d_{ij}}{v} * \eta \quad ... (2)$$

Formula 2

- d_{ij} : the distance between a vehicle i and a candidate RI j
- v: the average speed of vehicles (meter/second).
- η: the frequency of changing of pseudonym (pseudo/second).

We assume that v and η are fixed values. Thus, the objective function F can be rewritten as function of d ij as follows:

$$F = min \sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} x_{ij} \quad ... (3)$$

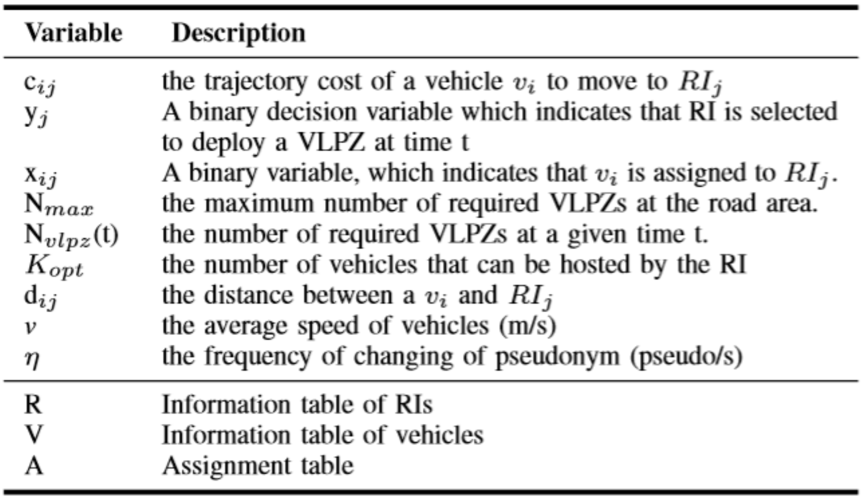
Formula 3

The feasibility of the solution depends on different constraints, which are represented by the following equations:

$$\begin{cases} \sum_{j=1}^{m} x_{ij} = 1 & ... (4) \\ \sum_{j=1}^{m} y_j = N_{vlpz}(t) & ... (5) \\ \sum_{j=1}^{n} x_{ij} <= K_{opt} & ... (6) \\ x_{ij} \in \{0,1\} & ... (7) \\ y_j \in \{0,1\} & ... (8) \end{cases}$$

Formula 4

(4) ensures that each vehicle v i is only assigned to one RI; (5) ensures that the number of selected RIs is equal to the number of VLPZ that are needed at time t (N vlpz (t)). (6) guarantees that the number of vehicles that are assigned to each infrastructure does not exceed the capacity of the RI(K opt); and finally, (7) and (8) are the integrity constraints. The description of variables is given in Table 11.



Variable	Description
c_{ij}	the trajectory cost of a vehicle v_i to move to RI_j
y_j	A binary decision variable which indicates that RI is selected to deploy a VLPZ at time t
x_{ij}	A binary variable, which indicates that v_i is assigned to RI_j.
N_{max}	the maximum number of required VLPZs at the road area.
$N_{vlpz}(t)$	the number of required VLPZs at a given time t.
K_{opt}	the number of vehicles that can be hosted by the RI
d_{ij}	the distance between a v_i and RI_j
v	the average speed of vehicles (m/s)
η	the frequency of changing of pseudonym (pseudo/s)
R	Information table of RIs
V	Information table of vehicles
A	Assignment table

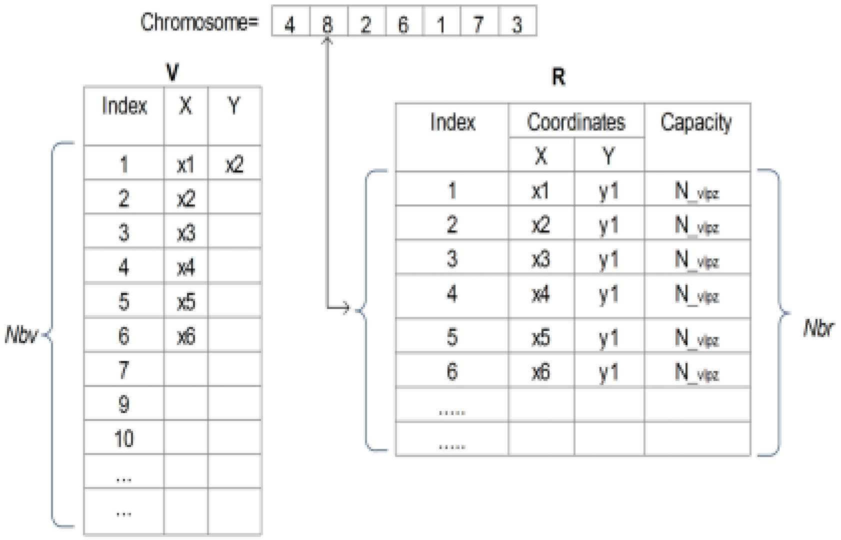
Table 11: The description of variables

3.4.2.3 VPGA: A Genetic Algorithm for an optimal placement of VLPZs

As shown in "Computers and Intractability; A Guide to the Theory of NP-Completeness", finding an optimal solution for the VLPZs placement is an NP-hard problem. Hence, we explore approximation techniques, and model the problem as finding the best fitted solution according to a genetic algorithmic model of the problem, after a fixed number of generations have been explored. In this vein, we propose a VLPZ Placement Genetic Algorithm (VPGA) for optimized placement of VLPZs within RIs. The pseudo-code of VPGA is illustrated in Figure 9. VPGA takes as input the current mobility information of vehicles and the positions of RIs and returns the VLPZs placement decision. In the following, the phases of VPGA are detailed.

A. Chromosome representation

In VPGA, each candidate solution is presented as a chromosome that is a chain of integers where each value is the index number of a potential RI. The length of the chromosome is equal to the optimal number of required VLPZs. As illustrated in Figure 8, the coordinates (x,y) and the capacities of the potential RIs are stored in R, which is a 2D Array (3 $*$ m). The vehicle coordinates are also stored in V, which is 2D Array(2*n). V is updated periodically according to the mobility of vehicles.



4	8	2	6	1	7	3

V

Index	X	Y
1	x1	x2
2	x2	
3	x3	
4	x4	
5	x5	
6	x6	
7		
9		
10		
...		
...		

R

Index	Coordinates		Capacity
	X	Y	
1	x1	y1	N_{vipz}
2	x2	y1	N_{vipz}
3	x3	y1	N_{vipz}
4	x4	y1	N_{vipz}
5	x5	y1	N_{vipz}
6	x6	y1	N_{vipz}
.....			
.....			

Figure 8: Chromosome representation

B. Initialization Phase

In this phase, the initial population of chromosomes is generated and vehicles are also assigned to each generated chromosome in order to compute the fittest chromosome. To cover the whole search space, the initial population is randomly generated. In addition, the size of the generated population is maintained in each iteration, which equals to the size of the initial population. However, a simple generation of the population could generate invalid chromosomes, which do not satisfy the constraint (4). For this reason, as described is Subroutine 1, for each generated gene, VPGA checks if it has already been added to the given chromosome or no. The random population procedure runs until the generation of all chromosomes. The assignment and the fitness calculation procedures are described in points 3.4.2.3 (F) and 3.4.2.3 (G), respectively.

C. Selection Phase

Selection is the first procedure to build a new population. A set of chromosomes from the old population should be selected to be parents for the rest of the procedures (crossover and mutation). VPGA uses two selection methods: elitism and tournament. Elitism selects the best fittest chromosomes from the old population and adds them to the new population. As described in Subroutine 2, VPGA only selects the best fittest chromosome and copy it to the newly created population. VPGA also uses the tournament method to select the parents that are used by the crossover to generate new chromosomes. The tournament selection method randomly chooses a set of chromosomes from the old population. The size of this set should be equal to the tournament size. After that, the fitness of each tournament chromosome is evaluated, and the fittest chromosome is selected as a parent for the crossover.

D. Crossover Phase

The crossover is a convergence operation that is used to generate new offsprings for the new population. It is intended to pull the population towards a local min or max. Crossover selects genes from the selected parents to create the new chromosome. As described in Subroutine 3, the crossover runs until the generation of the new population. In each iteration, a new chromosome is created based on the two parents chromosomes, which were selected using the tournament selection method. The genes of the new chromosome are selected using the uniform crossover i.e., the genes are randomly copied from the first or the second parent. The crossover computes the probability that determines from which parents the gene comes. Then the new chromosome is added to the new population.

E. Mutation Phase

Contrarily to crossover, the mutation is a divergence operation that is intended to occasionally break one or more members of a population out of a local min/max space and potentially discover a better space. The mutation operator works on a single chromosome. It aims to randomly introduce a new gene instead of inheriting it from the old chromosomes. The purpose is to avoid the local optimal covering the whole search space. As described in subroutine 4, the mutation runs until the generation of the new population. In each iteration, the genes of each chromosome are changed according to the mutation probability. This latter is used to determine whether the gene should be changed or not. In case a change is needed, a gene is randomly generated from the whole search space.

F. Assignment Phase

The next procedure after the generation or the update of the population is the assignment of vehicles to genes (RIs) of each chromosome in order to be able to evaluate the fitness. VPGA uses two algorithms of assignment: (i) The classical assignment: that calculates the Euclidean distance between each vehicle vi and each candidate RI, and (ii) The clustering-based assignment: that uses the K-means same size algorithm to create clusters of vehicles that have the same size, which equals to the capacity of the RI. The clustering-based assignment calculates the Euclidean distance between the cluster centroids and each candidate RI.

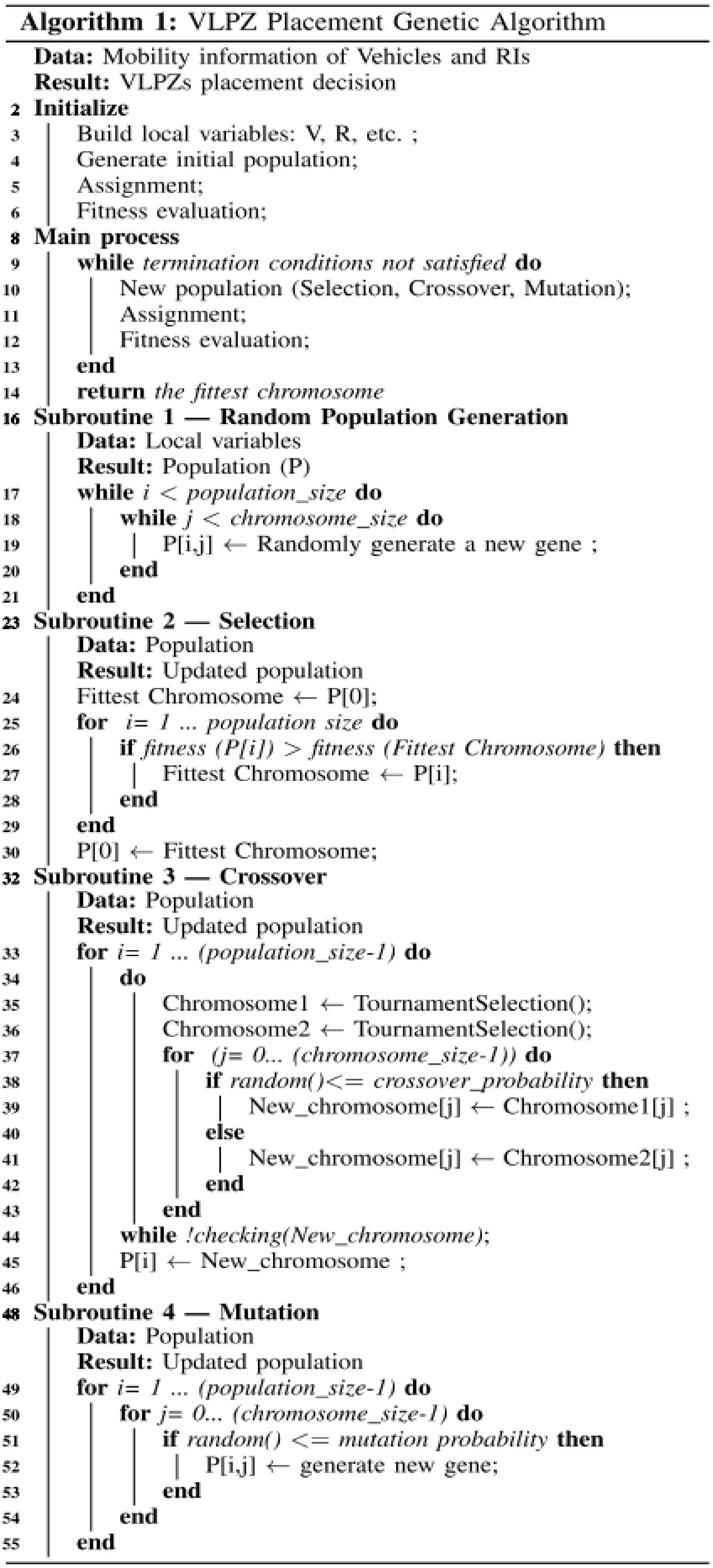
1. *Classical assignment***:** consists of three steps: (i) Compute the Euclidean distances between each vehicle vi and each candidate RI. These distances are saved in the distance table (D); (ii) Sort D from the lowest to the highest distance value; and (iii) Assign each vehicle to the nearest RI and save this assignment in A.
2. *Clustering-based assignment*: consists of four steps: (i) Create same-size clusters of vehicles. VPGA uses a variation of k-means clustering algorithm, proposed by ELKI Frame- work to create these clusters (Same-size k-means variation(ELKI Team, n.d.)); (ii) Calculate the distances between each centroid of a cluster and each candidate RI and save them in (D); (iii) Sort D from the lowest distance value to the highest one; and (iv) Assign each centroid to the nearest RI and save these assignments on A.

G. Fitness evaluation

Each generation of the genetic programming approach goes through mutations and crossovers. The newly generated solutions are evaluated according to a fitness function. We derive the fitness function according to the objective functions defined in the ILP formulation, namely equation (1).

H. Stop conditions

A genetic algorithm requires certain stop conditions to terminate. In VPGA, we consider two stop conditions related to two different aspects. The first condition is related to the convergence of our solution: if the fitness value keeps unchanged during three iterations, we assume that the optimal value of the fitness is reached, and the algorithm should be terminated. The second condition is linked to the number of iterations. We have simply limited the maximum number of iterations. VPGA returns the fittest chromosome i.e., the chromosome with the minimal fitness value.



```
Algorithm 1: VLPZ Placement Genetic Algorithm
Data: Mobility information of Vehicles and RIs
Result: VLPZs placement decision
Initialize
    Build local variables: V, R, etc. ;
    Generate initial population;
    Assignment;
    Fitness evaluation;
Main process
    while termination conditions not satisfied do
        New population (Selection, Crossover, Mutation);
        Assignment;
        Fitness evaluation;
    end
    return the fittest chromosome
Subroutine 1 — Random Population Generation
    Data: Local variables
    Result: Population (P)
    while $i <$ population_size do
        while $j <$ chromosome_size do
            P[i,j] ← Randomly generate a new gene ;
        end
    end
Subroutine 2 — Selection
    Data: Population
    Result: Updated population
    Fittest Chromosome ← P[0];
    for  i= 1 ... population size do
        if fitness (P[i]) > fitness (Fittest Chromosome) then
            Fittest Chromosome ← P[i];
        end
    end
    P[0] ← Fittest Chromosome;
Subroutine 3 — Crossover
    Data: Population
    Result: Updated population
    for i= 1 ... (population_size-1) do
        do
            Chromosome1 ← TournamentSelection();
            Chromosome2 ← TournamentSelection();
            for  (j= 0... (chromosome_size-1)) do
                if random()<= crossover_probability then
                    New_chromosome[j] ← Chromosome1[j] ;
                else
                    New_chromosome[j] ← Chromosome2[j] ;
                end
            end
        while !checking(New_chromosome);
        P[i] ← New_chromosome ;
    end
Subroutine 4 — Mutation
    Data: Population
    Result: Updated population
    for i= 1 ... (population_size-1) do
        for j= 0... (chromosome_size-1) do
            if random() <= mutation probability then
                P[i,j] ← generate new gene;
            end
        end
    end
```

Figure 9: VLPZ Placement Genetic Algorithm

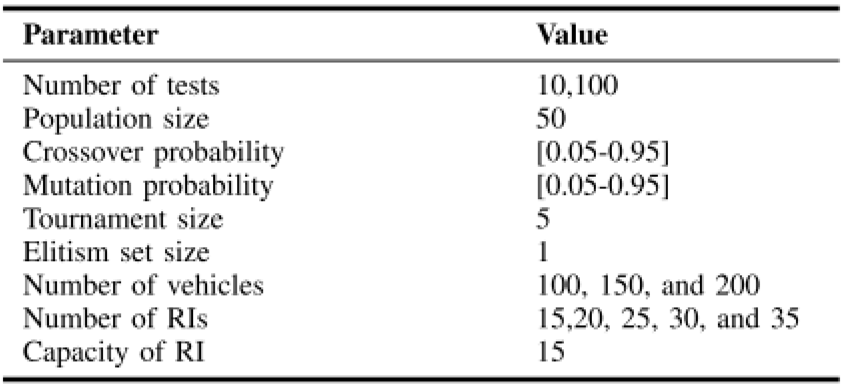
3.4.2.4 Numerical results

In this section, we evaluate the performance of VPGA considering the classical and clustering-based assignment. VPGA is one of the main functions of the vehicular SDN controller: optimal VLPZs placement. To show the merit of our approach, we compare it to the solution already proposed in PRIVANET (Boualouache et al. on PRIVANET, 2019). VPGA is programming and implemented using Java programming language and runon Intel i5 2.6 GHz. Table 6 shows the parameters used by VPGA. We have considered three levels of Vehicular Density (VD): Low (LVD), Medium (MVD), and High (HVD) for 100, 150, and 200 vehicles/km2 respectively. We varied also the number of RI from 15 to 35. The capacity of each RI is fixed to 15. We set the size of the generated population in each iteration to 50. The size of the chromosome of is calculated according to the following formula:

$$Chromosome\_size = \left\lceil \frac{Number\_Vehicles}{Capacity\_RI} \right\rceil$$

Formula 5

The performance of VPGA depends on the crossover and the mutation operators. For this reason, we fixed the tournament size and the elitism parameters to 5 and 1, respectively and varied the crossover probability and the mutation probability from 5% to 95%, respectively. Each test is repeated 10 times and the results are calculated with 95% of the confidence interval.



Parameter	Value
Number of tests	10,100
Population size	50
Crossover probability	[0.05-0.95]
Mutation probability	[0.05-0.95]
Tournament size	5
Elitism set size	1
Number of vehicles	100, 150, and 200
Number of RIs	15,20, 25, 30, and 35
Capacity of RI	15

Table 12: Simulation Parameters

- **Fitness Comparison**

Figure 10 compares the obtained fitness values using VPGA with its variations (classical and clustering-based assignments) and PRIVANET (Boualouache et al. 2019). In this evaluation, the position of vehicles and RIs are generated before the beginning of each iteration. We have considered the case of MVD and varied the number of RI from the lowest (15) to the highest value (35). As we can see, the best value of fitness is obtained when using VPGA with the classical assignment. The fitness decreases gradually when the number of RIs increases. This is due to the fact that with a large number of RIs, a high number of RIs will be in the vicinity of vehicles, hence the distances between vehicles and RIs are minimized.

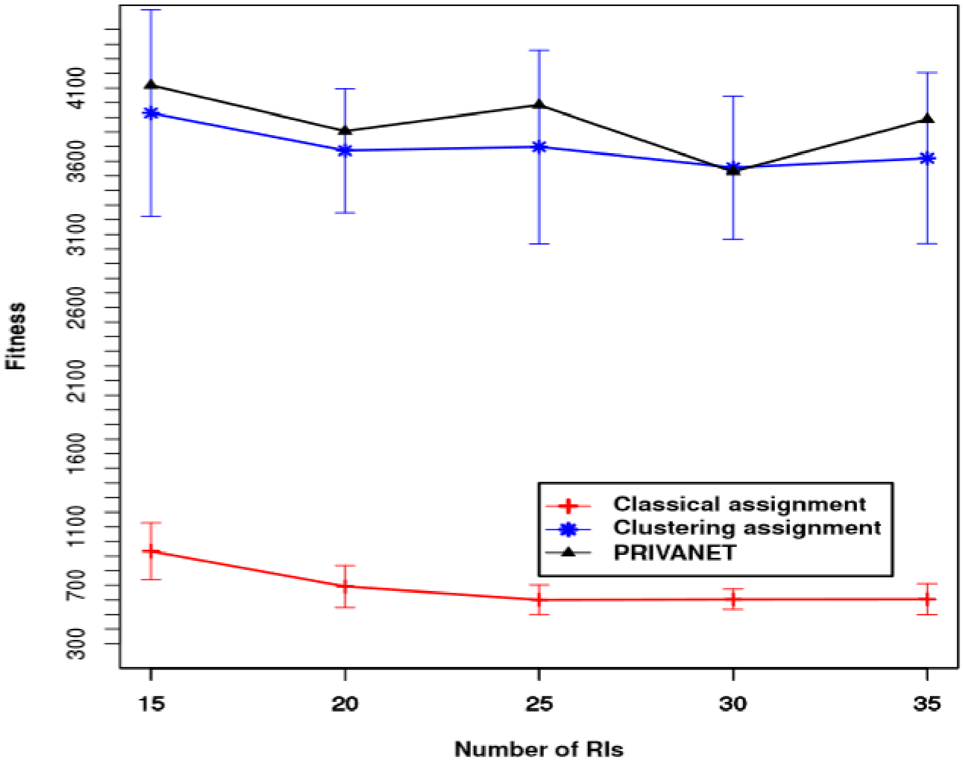


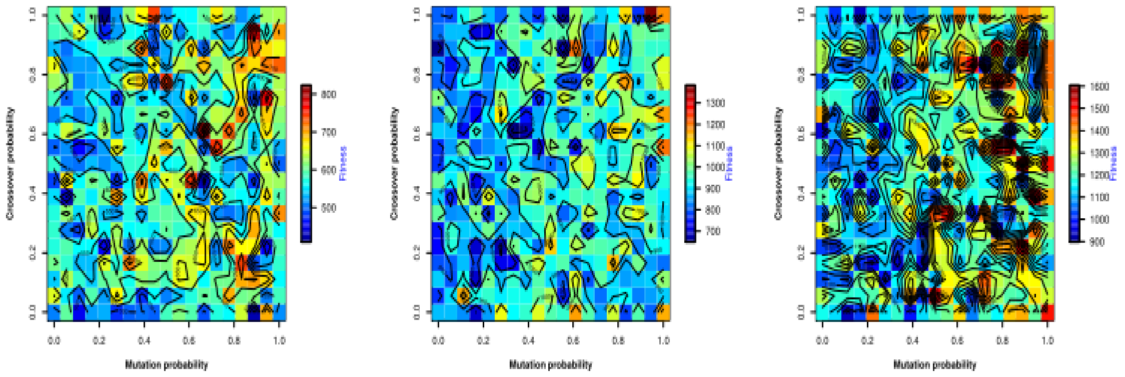
Figure 10: Fitness comparison under different approaches

- **Impact of vehicular density**

We evaluate in Figure 13, the fitness and the convergence speed obtained under different vehicles density (LVD, MVD, and HVD). As we can see in Figure 13a, the fitness decreases with the increase in the number of RIs for all VDs. For LVD and MVD, the fitness values approximately keep stable values between 25 and 35 RIs. However, for high densities, the value of fitness is enhanced in this interval. The reason for that with a high density of vehicles and with a large number of RIs, the distances between the vehicles and RIs will be short. As a result, the fitness value decreased. Figure 13b illustrates the speed convergence under different vehicle densities. We notice that the number of iterations increases with the number of RIs for all vehicle densities. Additionally, the convergence speeds of vehicle densities are close when the number of RIs is equal to 35. These results can be explained that with a large number of RIs, the search space of VPGA will be larger. Consequently, VPGA takes more iterations to reach the fittest chromosome, whatever the vehicle densities are.

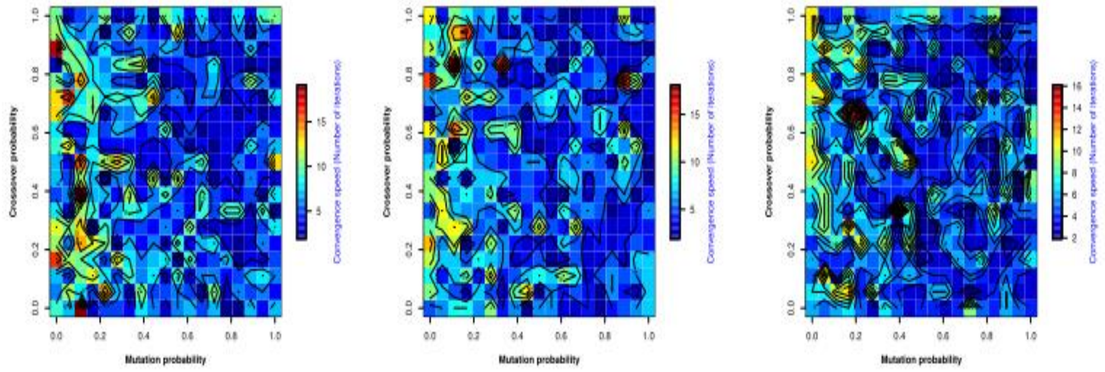
- **Parameters tuning**

We evaluate in Figure 11 and 12 the impact of the crossover probability and the mutation probability on the obtained fitness and convergence speed values, respectively under different VDs. The blue zones in the contour plots are the minimum values of fitness and convergence speed, respectively. We can see in Figure 11 that the density of the blue color is higher when the mutation probability between 5% and 20% and the crossover probability between 50% and 90%. Figure 12 shows that the density of the blue color is higher when the mutation probability is greater than 20%. To this end, the mutation and the crossover probabilities should carefully be tuned to establish the equilibrium between the fitness and convergence speed. In VPGA, the best results are obtained when the mutation probability equals 20% and the crossover probability ∈ [50, 90]%.



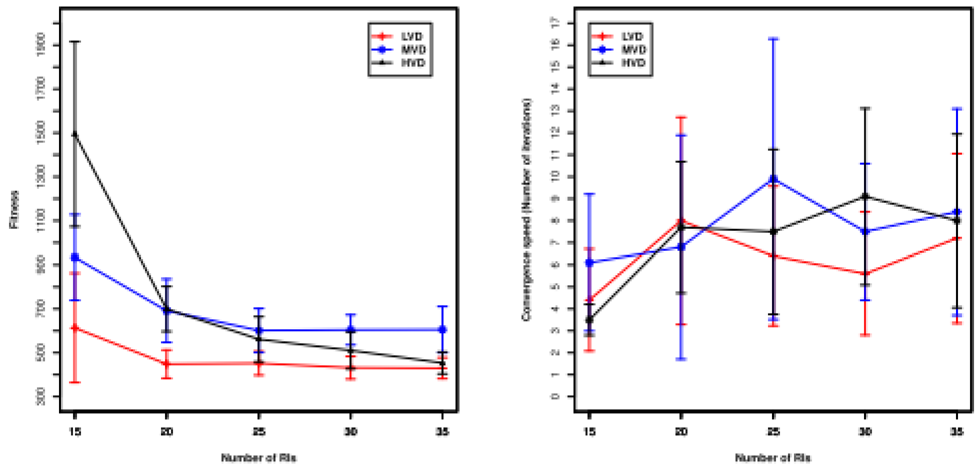
(a) LVD (b) MVD (c) HVD

Figure 11: Fitness evaluation with different crossover and mutation probabilities under different VDs



(a) LVD (b) MVD (c) HVD

Figure 12: Convergence speed evaluation with different crossover and mutation probabilities under different VDs



(a) Fitness. (b) Convergence speed.

Figure 13: Fitness and convergence speed comparison under different VDs.

- **Response time of the SDN controller**

To run adequately, VPGA needs an accurate input such as the number of RIs, densities of the traffic, coordinates of vehicles, etc. This input is provided by the SDN controller, which supervises the behavior of the moving vehicles via transmitted beacons and gets information about the RIs from authorities. In our SDN-enabled architecture, centralized control operations require less signaling traffic and shorter delays. When a change occurs in the network, the SDN knowledge is updated. Going further, we have compared the performances of our SDN-enabled architecture in terms of the response time of SDN controller under different vehicles densities. The response time is the time taken by the SDN controller to select the placement of the VLPZs. Recall that VLPZs placement is periodically calculated with SDN-controller. As shown in Figure 14, the response time increases with vehicular density. The maximal value is 7 seconds which is observed under HVD.

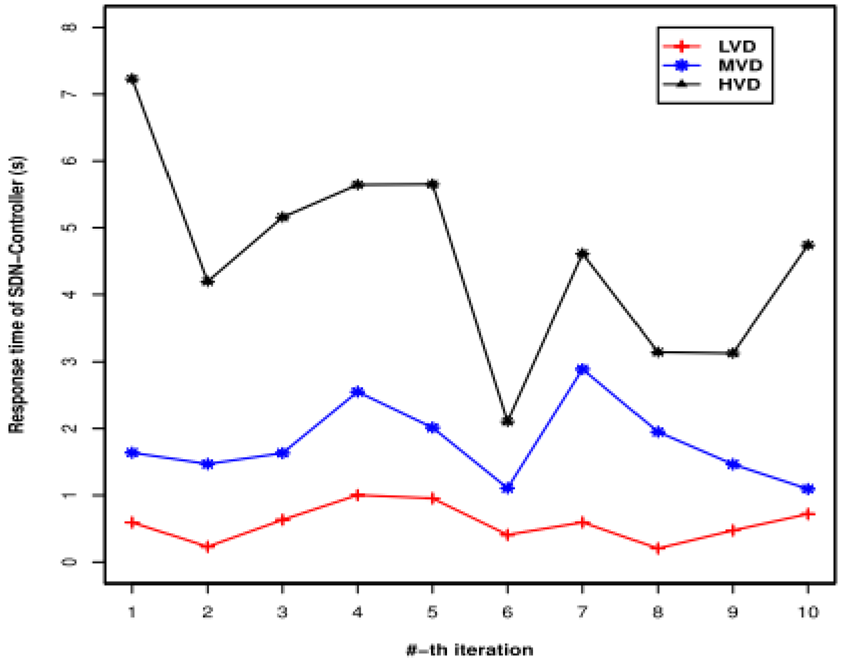


Figure 14: Response time of the SDN controller under different VDs

3.4.3 Situation-centric and dynamic misbehavior detection system for SDN-based 5G Vehicular Networks

Vehicular networks are vulnerable to a variety of internal attacks. Misbehavior Detection Systems (MDS) are preferred over the cryptography solutions to detect such attacks. However, the existing misbehavior detection systems are static and do not adapt to the context of vehicles. To this end, we exploit the Software-Defined Networking (SDN) paradigm to propose a context-aware MDS. Based on the context, our proposed system can tune security parameters to provide accurate detection with low false positives. Our system is Sybil attack-resistant and compliant with vehicular privacy standards. The simulation results show that, under different contexts, our system provides a high detection ratio and low false positives compared to a static MDS.

3.4.3.1 System model and MDS description

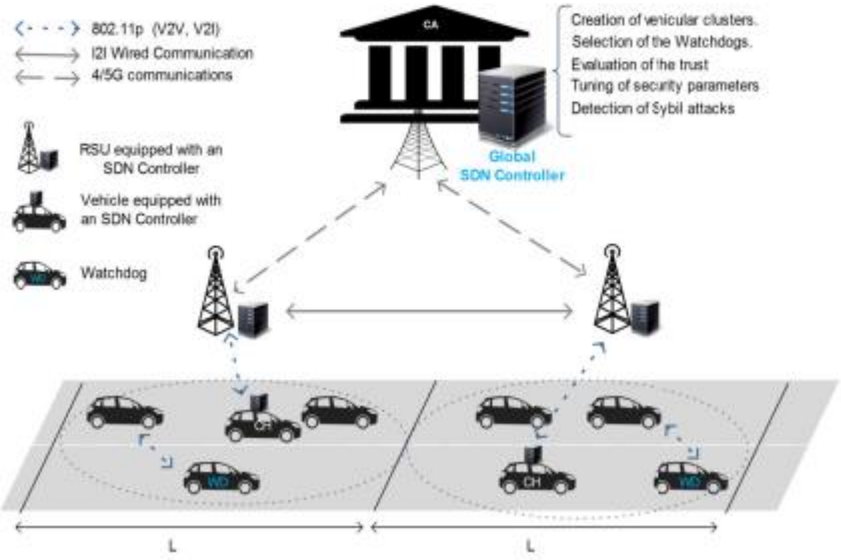

802.11p (V2V, V2I)
I2I Wired Communication
4/5G communications
RSU equipped with an SDN Controller
Vehicle equipped with an SDN Controller
Watchdog
CA
Global SDN Controller
Creation of vehicular clusters.
Selection of the Watchdogs.
Evaluation of the trust
Tuning of security parameters
Detection of Sybil attacks
CH
WD
CH
WD
L
L

Figure 15: Software-defined vehicular network architecture for MDS

As illustrated in Figure 15, we consider a software-defined vehicular network architecture consisting of vehicles, Road Side Units (RSUs), and the Certification Authority (CA). This architecture has three levels of SDN control: (i) Local SDN controllers, which are installed on each Cluster Head (CH). The role of these controllers is to select the Watchdogs according to the strategy described in Section IV-B and to calculate the trust level of Cluster Members (CMs); (ii) Regional SDN controllers, which are installed on RSUs. These controllers calculate trust levels of local SDN-controllers and aggregate the trust level of vehicles; and (iii) Global SDN controller, which is installed at the CA and has global knowledge of the software-defined vehicular network. The global SDN-controller creates the vehicular clusters, selects CHs (see Section IV-A) tunes the security parameters of the MDS. Vehicles except the CHs belong to the forwarding plane. Each vehicle is equipped with an IEEE 802.11p interface to communicate with other vehicles. Each vehicle is also equipped with an SDN controller and an SDN agent. This agent is always activated. However, the SDN controller is initially deactivated and will only be activated when the vehicle becomes a CH and deactivated again if the vehicle reverts to a CM. Each RSU is equipped with two interfaces: a wired link to communicate with the neighboring RSUs, and an LTE/5G interface to communicate with the global SDN controller. We assume that the RSUs are trusted nodes and the communication links between the local SDN controllers, the vehicles, and between the three types of SDN controllers are secured.

In our proposed SDN-based MDS system, the control plane five main control functions: (i) Creation of vehicular clusters;(ii) Selection of the Watchdogs; (iii) Evaluation of the trust; (iv) Detection of Sybil attacks; and (v) Tuning of security parameters including not only the parameters and thresholds of the trust, but also the number of Watchdogs. A Watchdog monitors the neighboring vehicles and sends its reports to the local SDN-controller. The local SDN controller monitors all CMs and calculates their trust levels leveraging on their monitoring reports and the reports received from Watchdogs. Finally, the local SDN controller sends its report to the regional SDN controller. This latter monitors local SDN- controllers and calculates their trust levels. Then, the regional SDN controllers aggregate all the trust values of vehicles and send the final report to the global SDN-controller. This process is periodically executed during the evaluation period.

3.4.3.2 Clustering and watchdogs election

Clustering Strategy

We assume that the road is divided into equal static segments as shown in Figure 14. The length of the segment (L) is less than the communication range of vehicles (R). We assume that the global SDN controller periodically creates the vehicular clusters, which are restrained to these segments. Indeed, at a given time t, all vehicles within a given segment are all considered members of the same cluster and the cluster head is selected according to the Selection Factor (SF), which is given by the formula:

$$SF_i = \alpha * Trust_i + \beta * (Ndistance_i * Nspeed_i)$$

Formula 6

$$Ndistance_i = \frac{Maxdistance - distance_i}{Maxdistance}$$

Formula 7

$$Nspeed_i = 1 - \frac{|speed_i - Avgspeed|}{Maxspeed - Minspeed}$$

Formula 8

Formula (2) selects the most honest and stable vehicle to become the CH. A vehicle i is stable if it is close to the center of the cluster and its speed is close to the average speed of all CMs of the same cluster. For this reason, the selection of the CH is based on two criteria: trust ($Trust_i$) and mobility.

The impact of each of these criteria is weighted by α and β (α + β = 1, α,β ∈ [0, 1]). The mobility is measured according to: (i) $Ndistance_i$ (calculated by the formula (3)), which is the normalized value of the distance between the vehicle and the center of the segment, and (ii) $Nspeed_i$ (calculated by the formula (4)), which is the normalized value of the difference between the vehicle's speed and the average speed of the CMs. The vehicle with the highest SF value is selected as a CH. We assume that the cluster management (the creation and the update of clusters) is performed by the global SDN-controller.

Watchdogs Election

The evaluation of the trust of a vehicle is computed based on the opinions collected from his neighbor vehicles, namely watchdogs. However, it is crucial to ensure that opinions are not collected from misbehaving Watchdogs. In addition, a significant overhead could be generated if a large number of vehicles plays the role of a watchdog. For these reasons, the local SDN-controller should carefully select the Watchdogs according to their trust level and their distance to vehicles. To this end, we propose that the number of Watchdogs should be determined by the formula (5) where z is the size of the cluster and ρ_w is the density of the watchdogs. The density of watchdogs is determined as functions of the presence the misbehaving vehicles.

$$nbr_{watchdogs} = \frac{z}{\rho_w}$$

Formula 9

After the calculation of the number of Watchdogs, we deploy them according to the number of road lanes and the distribution of vehicles on the considered segment. The segment is thus divided into zones whose number (nbr_{zone}) is calculated using the following formula:

$$\begin{cases} nbr_{zone} = nbr_{lanes} & if(nbr_{lanes})\%2 = 0 \\ nbr_{zone} = nbr_{lanes} + 1 & else \end{cases}$$

Formula 10

with nbr_{lanes} denotes the number of lanes. The number of Watchdogs that can be deployed at each zone ($nbr_{watchdogs/zone}$) can be calculated using the formula (11). The vehicles with high trust values in each zone are selected as Watchdogs.

$$nbr_{watchdogs/zone} = \frac{nbr_{vehicle/zone}}{\rho_w}$$

Formula 11

3.4.3.3 Trust Computation and SYBIL Attack Resistance

Trust computation

The trust of Vehicles (CMs) is evaluated by the local SDN controller based on their actions. The trust level of a vehicle is divided into two parts: the direct and the indirect trust. The direct trust is calculated based on the interactions between the vehicle and the local SDN controller (CH), whereas indirect trust is calculated based on interactions of the vehicle and the Watchdogs. The trust level of a given vehicle v ($Trust_v$) is thus given by the following formula:

$$Trust_v = (1 - \frac{1}{(\gamma * I_v) + 1}) * DT_v + (\frac{1}{(\gamma * I_v) + 1}) * IT_v$$

Formula 12

Where Iv is the number of direct interactions between the vehicle and the local SDN controller. Since the direct trust is more important in the calculation of the trust, we assign more weight to it (1 − 1 / (γ ∗ I)+1), which rapidly increases with the number of direct interactions (Iv). However, it is controlled by the parameter γ ∈ R+.

Direct Trust

Direct trust is computed based on the actions of the vehicle during its journey. An action can be either honest or misbehaving. A misbehaving action in our model is defined as a malicious action performed by misbehaving vehicles such as a message drop, false information injection, message replay and channel jamming. The impact of these misbehaving actions is different. For example, injecting false information is more harmful than replaying a message (Ahmad et al. 2018). For this reason, we introduce a weight s_j ∈ {1: Low, 2: Medium, 3: High, 4: Lethal} for each misbehaving action to reflect its impact on the safety. To this end, we denote by (A^h_v) and A^m_v, the number of honest actions performed by a vehicle v and the number of weighted misbehaving actions given by the formula (13), respectively. The total number of weighted actions A_v is the sum of honest actions and weighted misbehaving actions as given in the formulas.

$$A_v^m = \sum_{j=1}^{n} s_j * A_j$$

Formula 13

$$A_v = A_v^h + A_v^m$$

Formula 14

The direct trust is thus calculated using the following formula (15).

$$DT_v = \frac{A_v^h}{A_v} * \frac{1}{\gamma * A_v^m + 1}$$

Formula 15

Indirect Trust

The indirect trust of a vehicle v is the average of trust levels calculated by the watchdogs who were interacting with them. The indirect trust of a vehicle is thus calculated using the formulas (16), where nbrw is the number of Watchdogs who have interacted with v and DTw k v is the direct trust of a vehicle v calculated by a Watchdog k using the formula (15).

$$IT_v = \frac{1}{nbr_w} \sum_{k=1}^{nbr_w} DT_v^{w_k}$$

Formula 16

- **Trust computation of local SDN-controllers**

Local SDN controllers (CHs) are also evaluated by the regional SDN controller based on their actions. The trust level of a local SDN controller (LT) is thus the average of direct trust levels of regional SDN controllers who have interacted with it. It is hence given by the formula (17), where nbr_{rc} is the number of regional SDN controllers and DT^{rci}_{v} is a direct trust level reported by a regional SDN controller rc_i. DT^{rci}_{v} is defined by the formula (18).

$$LT = \frac{1}{nbr_{rc}} \sum_{i=1}^{nbr_{rc}} DT_{lc}^{rc_i}$$

Formula 17

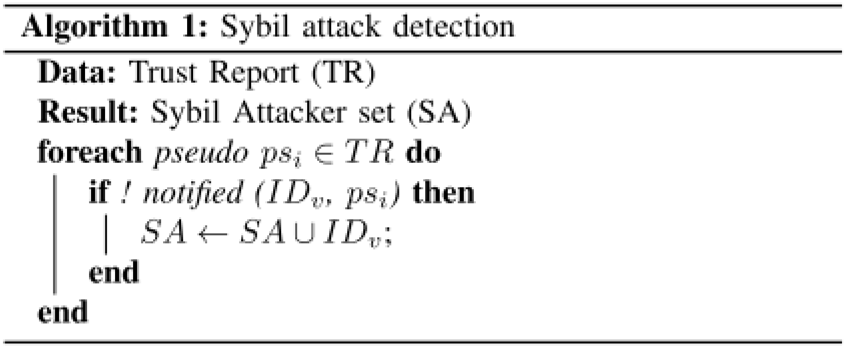
$$DT_{lc} = (\frac{A_{lc}^m}{A_{lc}}) * (1 - \frac{1}{(\gamma * A_{lc}) + 1})$$

Formula 18

Where A^{m}_{lc} is the number of weighted misbehaving actions performed by the local SDN controller, while A_{lc} is the total number of weighted actions.

- **Aggregation, privacy and Sybil attack resistance**

In our MDS, the trust levels of vehicles are regularly calculated according to a fixed time period Δ, which is dynamically adjusted by the global SDN controller. During Δ, the local SDN controller (CH) calculates the direct trust levels of its cluster members and each Watchdog calculates the trust levels of its neighbouring CMs. At the end of Δ, each Watchdog reports the calculated direct trust levels to the local SDN controller. As soon as these reports are received, the local SDN controller calculates the final trust level of all its CMs. These calculated trust levels (trust report) are sent to the global SDN-controller (CA) via regional SDN-controllers (RSUs). The CA thus decides the truthfulness of vehicles if the trust of the vehicle is below a trust threshold σ ∈ [0, 1]. This threshold is dynamically adjusted by the SDN-controllers to provide high detection accuracy and to decrease the false positive.



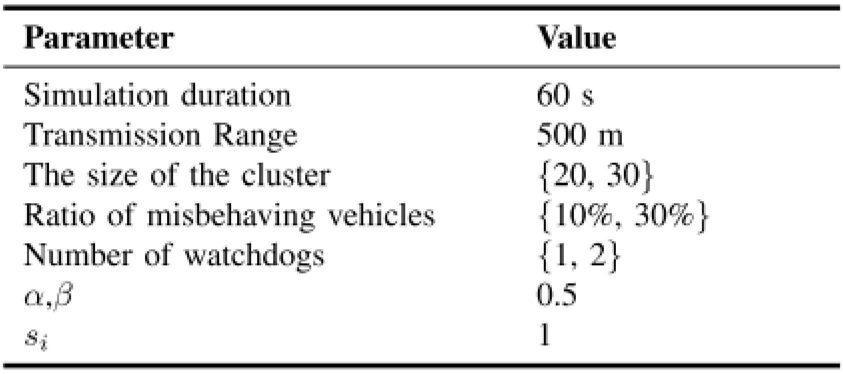
```
Algorithm 1: Sybil attack detection
Data: Trust Report (TR)
Result: Sybil Attacker set (SA)
foreach pseudo $ps_i \in TR$ do
    if ! notified $(ID_v, ps_i)$ then
        $SA \leftarrow SA \cup ID_v$;
    end
end
```

Figure 16: Sybil attack detection

However, as vehicles frequently change their pseudonyms, different trust values associated with the same vehicle could be reported to the CA. In addition, misbehaving vehicles could use their pseudonyms as Sybils to avoid being detected. To overcome this problem, we propose that each vehicle notifies its local SDN-controller before changing its pseudonym. This notification is forwarded to the global SDN controller (CA). Each time the CA receives a trust report, it runs the Sybil attack detection algorithm as described in Figure 16. For each reported trust level entry, the CA checks if the used pseudonym psi was reported or not using its long-term identity ID_v. If a vehicle v changes its pseudonym without informing the CA, it is considered as a misbehaving vehicle and added to the Sybil attacker list.

3.4.3.4 Performance Evaluation

We have carried out a set of simulations to evaluate the performance of our proposed MDS. These simulations are conducted using Veins Simulation Framework (Sommer et al. 2011). Table 13 summarizes the simulation parameters.



Parameter	Value
Simulation duration	60 s
Transmission Range	500 m
The size of the cluster	{20, 30}
Ratio of misbehaving vehicles	{10%, 30%}
Number of watchdogs	{1, 2}
α,β	0.5
s_i	1

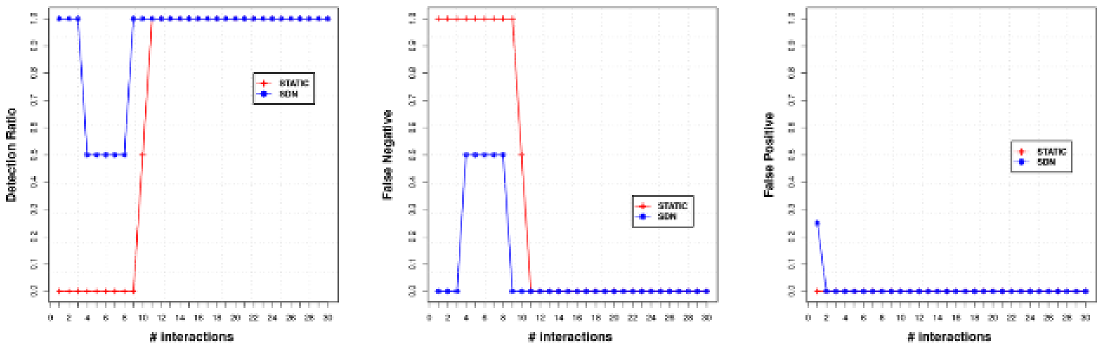
Table 13: Simulation Parameters

We considered the case of a free-way road. We simulated a 2-lane straight road section of 3 Km. The mobility of vehicles is generated using SUMO. As shown in Table 13, we considered the case of medium clusters (20 to 30 vehicles). We also considered low (10%) and high (30%) ratio of misbehaving vehicles. The parameters α and β are fixed to 0.5, while the weight of all misbehaving actions (s_j) equals to 1. We studied the efficiency of the proposed MDS in general, but in particular, we evaluated the merit of introducing the SDN in our proposed system. For this reason, we considered two versions of our proposed MDS: (i) the Static-MDS: this is a free-SDN version, which uses a default configuration (nbr_w = 2, σ = 0.5, γ = 1) that does not change over time and do not adapt to the context of vehicles; and (ii) SDN-MDS: which was described in the previous sections and ensures the implementation of an adaptive MDS. In this version, the security parameters of the MDS (nbr_w, σ, and γ) are changed according to the context of vehicles. By mixing up the ratio of attackers and the the size of cluster, we came up with 4 different contexts. During the evaluation period, 30 interactions between the local SDN controllers and the Watchdogs were performed.

	Size of Cluster	Ratio of misbehaving Vehicles	nbr_w	σ	γ
Context 1	20	10%	1	0.55	1.5
Context 2		30%	1	0.6	1
Context 3	30	10%	1	0.67	1.5
Context 4		30%	1	0.7	1.5

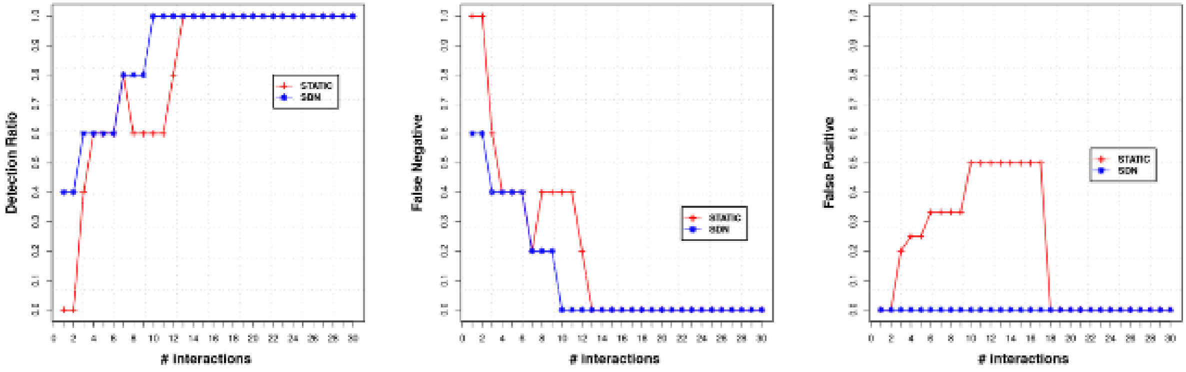
Table 14: Context Parameters

Figure 17, Figure 18: Context 2, Figure 19: Context 3, and Figure 20: Context 4 compare the performances of Static-MDS and SDN-MDS in terms of detection ratio, false negative, and false positives in each considered context. It is clear that our proposed MDS provides early and accurate detection of the attack. In addition, we can see that SDN-MDS adapts the security parameters (nbrw, σ, and γ) according to the context to enhance the detection ratio and decrease the false negative/positive as the number of interactions increase. As shown in Table 14, compared to the static version, only 1 Watchdog is deployed by the SDN controller because the attackers are grouped only on one side of the clusters. However, the values assigned to the parameter γ show that the SDN controller generally puts much consideration on the direct trust evaluation provided by the local SDN controller compared to the indirect trust evaluation provided by the Watchdogs as the number of attackers increases. Table 8 also shows that the trust threshold (σ) is also adapted in each considered context to provide high detection radio with a low negative/positive rate.



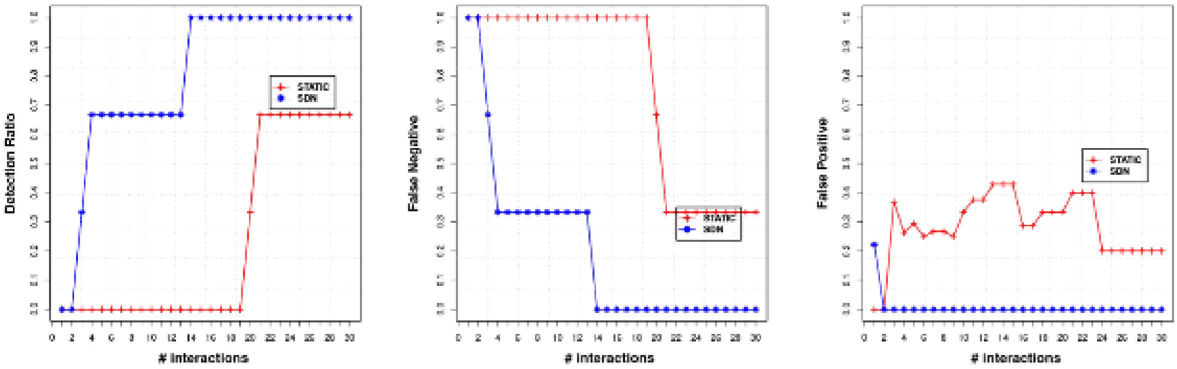
(a) Detection ratio (b) False negative (a) False positive

Figure 17: Context 1



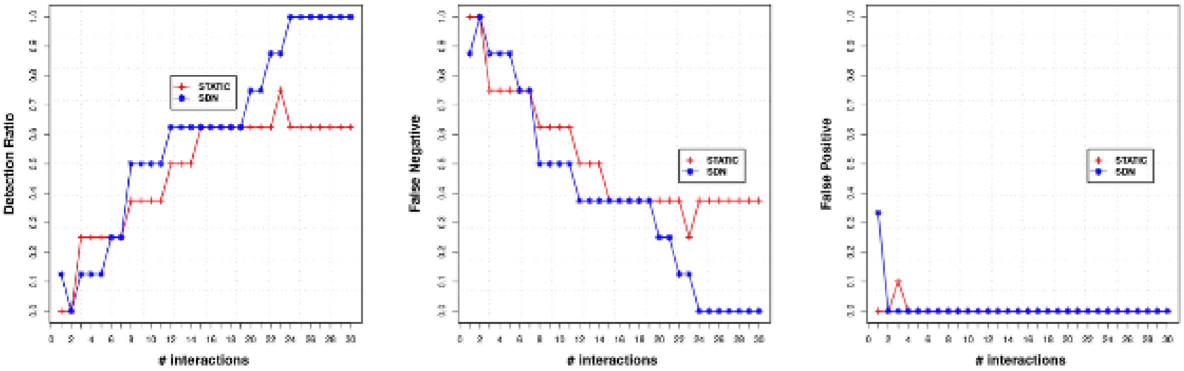
(a) Detection ratio (b) False negative (a) False positive

Figure 18: Context 2



(a) Detection ratio (b) False negative (a) False positive

Figure 19: Context 3



(a) Detection ratio (b) False negative (a) False positive

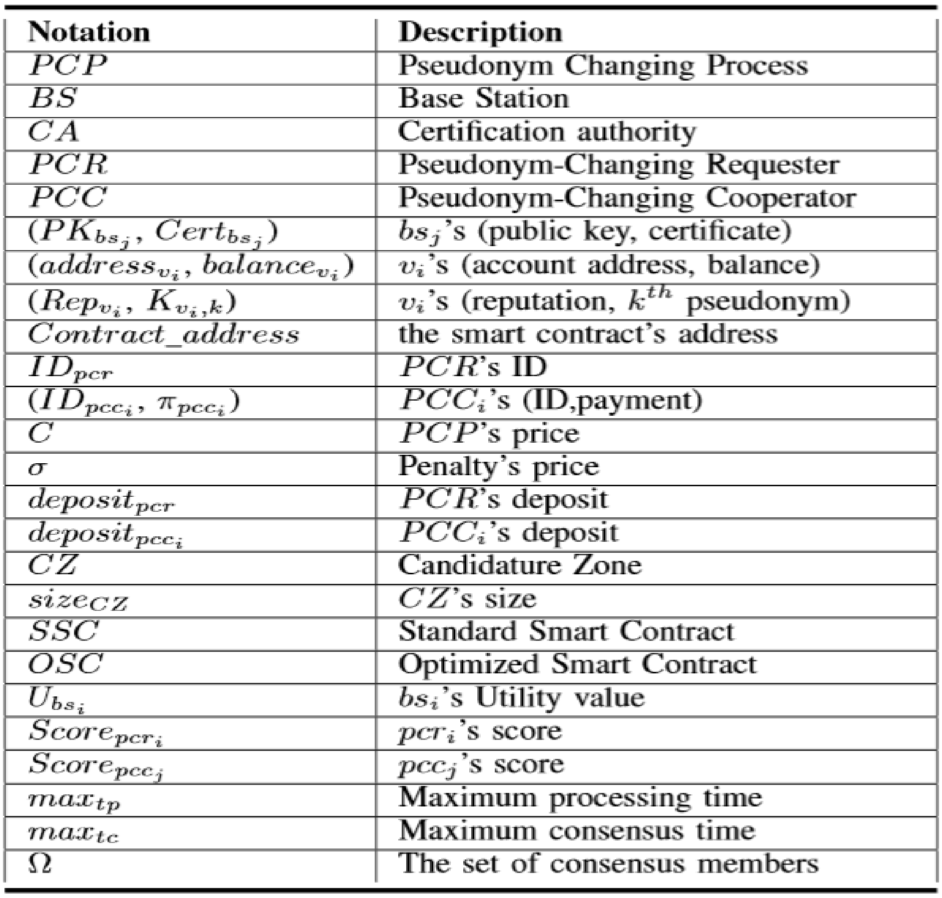
Figure 20: Context 4

3.4.4 Blockchain for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing

Privacy is a key requirement for connected vehicles. Cooperation between vehicles is mandatory for achieving location privacy preservation. However, non-cooperative vehicles can be a big issue to achieve this objective. To this end, we propose a novel monetary incentive scheme for cooperative location privacy preservation in 5G-enabled Vehicular Fog Computing. This scheme leverages a consortium blockchain-enabled fog layer and smart contracts to ensure a trusted and secure cooperative Pseudonym Changing Processes (PCPs). We also propose optimized smart contracts to reduce the monetary costs of vehicles while providing more location privacy preservation. Moreover, a resilient and lightweight Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus protocol is proposed to ensure fast and reliable block mining and validation. The performance analysis shows that our scheme has effective incentive techniques to stimulate non-cooperative vehicles and provides optimal monetary cost management and secure, private, fast validation of blocks.

3.4.4.1 Blockchain-based architecture for cooperative location privacy preservation

In this section, we present our blockchain-based architecture for cooperative location privacy preservation in 5G-enabled vehicular fog computing. This section is structured as follows. We first describe the considered system model. We then present the system's initialization. Finally, we describe the attacker model. Table 15 presents the used abbreviations and notations.



Notation	Description
PCP	Pseudonym Changing Process
BS	Base Station
CA	Certification authority
PCR	Pseudonym-Changing Requester
PCC	Pseudonym-Changing Cooperator
$(PK_{bs_j}, Cert_{bs_j})$	bs_j's (public key, certificate)
$(address_{v_i}, balance_{v_i})$	v_i's (account address, balance)
$(Rep_{v_i}, K_{v_i,k})$	v_i's (reputation, k^{th} pseudonym)
$Contract\_address$	the smart contract's address
ID_{pcr}	PCR's ID
$(ID_{pcc_i}, \pi_{pcc_i})$	PCC_i's (ID,payment)
C	PCP's price
σ	Penalty's price
$deposit_{pcr}$	PCR's deposit
$deposit_{pcc_i}$	PCC_i's deposit
CZ	Candidature Zone
$size_{CZ}$	CZ's size
SSC	Standard Smart Contract
OSC	Optimized Smart Contract
U_{bs_i}	bs_i's Utility value
$Score_{pcr_i}$	pcr_i's score
$Score_{pcc_j}$	pcc_j's score
max_{tp}	Maximum processing time
max_{tc}	Maximum consensus time
Ω	The set of consensus members

Table 15: Abbreviations and notations

A. System Model

As illustrated in Figure 21, we consider a 5G-enabled vehicular fog computing architecture consisting of two layers. The infrastructure layer includes vehicles equipped with V2X technology. In this layer, communications are multi-hop Vehicle-to-Vehicle (V2V). Vehicle-to-Infrastructure (V2I) communications are only used to communicate with the 5G-fog layer. This latter consists of several Base Stations (BSs) acting as fog nodes with sufficient data storage, processing, and computing capabilities, and distributed over a specific geographic perimeter. All BSs are connected through secure 5G links. We also consider that each bs$_j$ is equipped with a consortium blockchain hosting transactions and SCs for enabling secure cooperation between vehicles. Vehicles should carry out coordinated PCPs to protect their location privacy. They can then request PCPs from their neighbors. However, they cannot be sure that their neighbors will cooperate with them, which leads to the failure of PCPs. Consequently, vehicles may ask for support from our scheme. Indeed, 5G blockchain-based fog layer is acting as a controller of PCPs. All vehicles involved in these PCPs are protected by SCs, while cooperation transactions are recorded in the consortium blockchain. In the following, we define a Pseudonym-Changing Requester (PCR)as each vehicle requests to perform a PCP i.e it requests to change its pseudonym with the neighboring vehicles. We also define a Pseudonym-Changing Cooperator (PCC) as each vehicle that participates in a PCP. The fog layer allows the rapid processing of the PCP's procedure from the PCR's request to the execution of the SC.

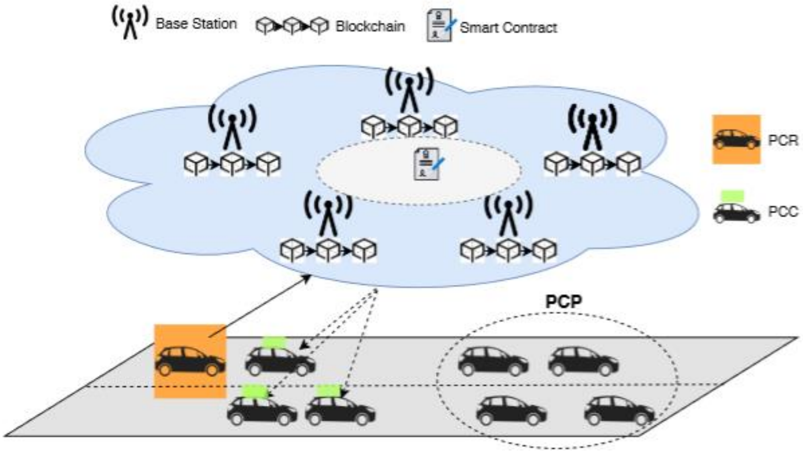


Figure 21: Blockchain-based architecture for cooperative location privacy preservation in 5G-enabled vehicular fog computing

B. System Initialization

To implement efficient cooperation between vehicles, before joining to the systems, vehicles and BSs register with the Certification Authority (CA). Specifically, during the registration, each bsj is equipped with a legitimate identity consisting of a private key $SK_{bs}j$, a public key $PK_{bs}j$, and a public certificate $Cert_{bsj}$, respectively. On the other hand, each vehicle vi is equipped with a legitimate identity consisting of a private key SK_{vi}, a public key PK_{vi}, and a public certificate $Cert_{vi}$, respectively. Each vehicle vi also gets an account $account_{v}i$, which includes its wallet address $address_{vi}$, its account balance $balance_{vi}$, its reputation value Rep_{vi}. Moreover, each vehicle vi is pre-loaded with a set of s pseudonyms $K_{vi,k}$ where k ∈1, ..., s, which are public keys certified by the CA. For each pseudonym $K_{vi,k}$, the CA provides a certificate $Cert_{vi,k}(K_{v}i,k)$. To ensure the authentication and integrity of information, asymmetric encryption is used in the architecture. Safety messages are properly signed with a private key $K^{-1}_{vi,k}$ corresponding to the pseudonym $K_{vi,k}$. A certificate is attached to each message to enable other vehicles to verify the sender's authenticity. In addition, each entity (vehicle/BS) is equipped with a security defense agent for thwarting internal attacks defined in subsection 3.4.4.1 (C). Each vehicle periodically broadcasts a safety message every t millisecond, where each message includes a location, a timestamp, a velocity, Anda content. On the other hand, to maintain the privacy of vehicles in the blockchain, pseudonyms considered as the source address for verifying the authenticity of transactions. Pseudonyms are also used as account addresses. To this end, only CA still knows the relationship between the real identifier of the vehicle and its corresponding pseudonyms.

C. Attack Model

Malicious entities (vehicles/BSs) can have a significant impact on the scheme. In the following, we identify three types of attackers.

1. *Malicious PCR*: a malicious PCR can request to execute a PCP without having enough money in its balance or it can pretend that one or several PCC(s) did not change its/their pseudonym(s) in the PCP.
2. *Malicious PCC*: to be rewarded, a malicious PCC can pretend that it changes its pseudonym in PCP, but in reality, it did not.
3. *Malicious BS*: a malicious BS tries to tamper PCP's related information such as reputations

and data received from vehicles to increase its benefits.

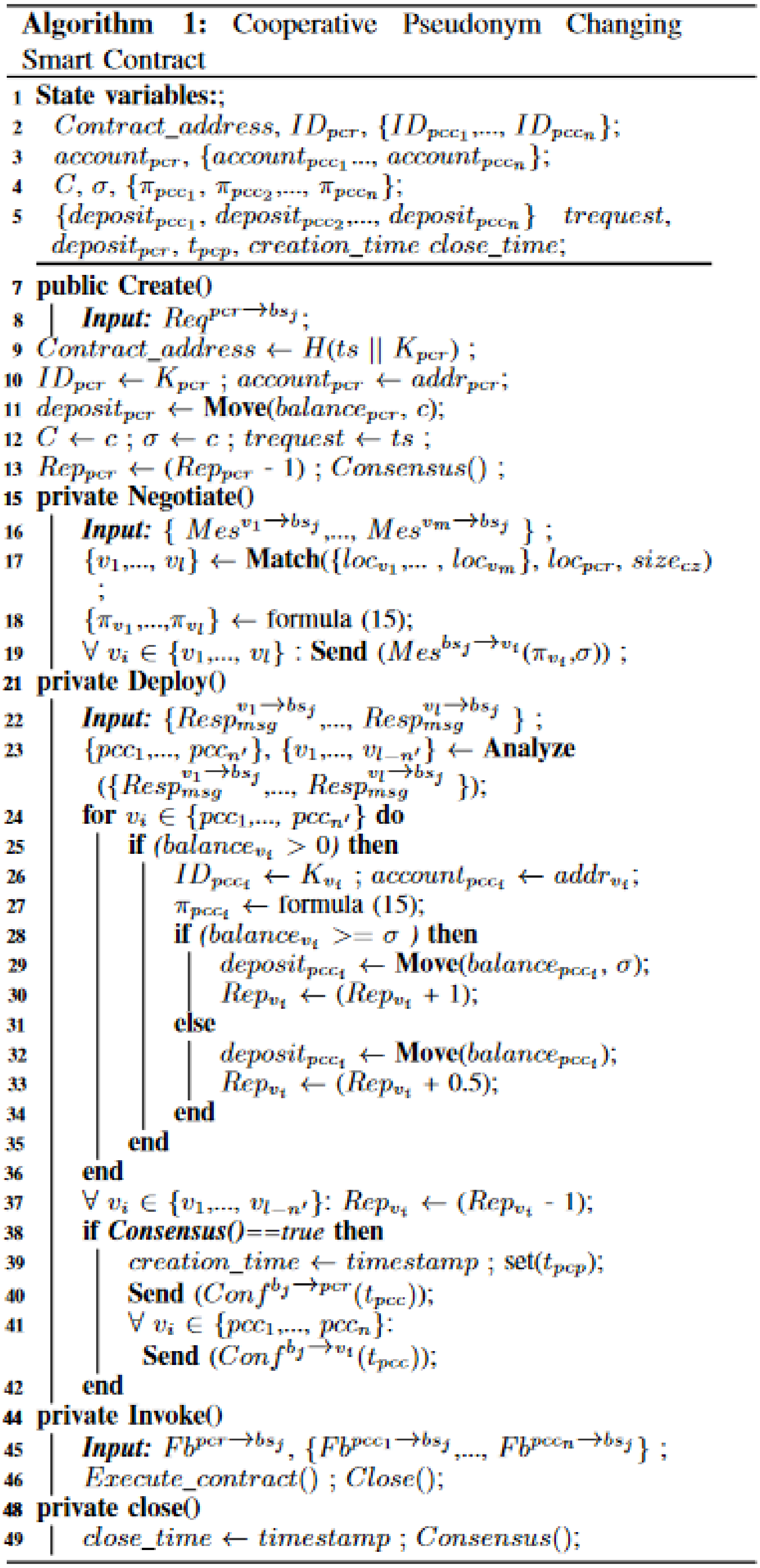
Malicious entities can launch internal and denial of service attacks. They can also launch more advanced attacks like strategic attacks, where attackers disguise as PCCs first and then timely switch to malicious behaviors to threaten the proposed scheme.

3.4.4.2 Cooperative Pseudonym Changing Smart Contract

In this section, we design a SC aiming at ensuring trust cooperation between vehicles and stimulating them to participate in PCPs. Each SC has a unique contract address (Contract_address) and maintains a set of state variables including the identifier of the PCR (ID_{pcr}), the account address of the PCR ($account_{pcr}$), the identifiers of PCCs {ID_{pcc1},...,ID_{pccn}}, the account addresses of PCCs {$account_{pcc1}$,...,$account_{pccn}$}, the price of the PCP C .i.e the total number of coins the PCR that pays for the PCCs. The contract also includes the number of coins to pay for each PCC {π_{pcc1},...,π_{pccn}}, the penalty price (σ) applied to a PCC in case of noncooperation, ρ is the service ratio to calculate the number of coins to pay network operators managing BSs from C, the time when a PCR requests the creation of the smart contrat (trequest), the time when the SC is effectively created (creationtime), the time when the PCP is performed (tpcp), and the closing time of the SC (closetime). In addition, to protect against malicious PCR and PCCs, the PCR and each PCC should move a deposit from their wallet addresses to the contract address. Specifically, the PCR and PCCs should move numbers of coins to ($deposit_{pcr}$) and {$deposit_{pcc1}$,...,$deposit_{pccn}$} respectively. Figure 22 describes the implementation of the SC. The pseudonym changing SC consists of one public function, which can be called by vehicles, and four private functions, which can only locally be called by the BS.

A. Create

When a vehicle vi (PCR) wants to execute a PCP, it needs to call the create function. Thus, it sends a request to the nearest bsj: Req $^{pcr-\rightarrow bsj}$=EPKbsj (addrpcr || c || locpcr || Kpcr || SigKpcr || CertKpcr || ts). This request is encrypted by P Kbsj and includes the PCR's account address (addrpcr), the price to pay to perform this operation (c), the current location (locpcr), PCR's current pseudonym (Kpcr), the corresponding signature (Sig(Kpcr)), certificate (CertKpcr), and a timestamps. Once bsj receives a request from a PCR,it first checks Reppcr and balance pcr to verify if its reputation is positive and it has enough coins to pay for PCCs and service fees in step (9). If the condition is satisfied, the SC is created and a unique identifier is assigned to the contract address in step (10), which consists of the hash value of the concatenation of the timestamp and the current pseudonym of the PCR. The state variables (IDpcr and accountpcr) related to PCR are also initialized in step (11) and a deposit of c coins is moved from balancepcr to depositpcr in step (12). C,σ, and trequest are also initialized in step (13). However, if the PCR tries to execute a PCP without having enough coins in its balance, the request is refused, and the reputation value of the PCR is decreased in step (15). A consensus process should also be done latter to update the blockchain ledger.



Algorithm 1: Cooperative Pseudonym Changing Smart Contract

```
State variables:;
  $Contract\_address, ID_{pcr}, \{ID_{pcc_1},..., ID_{pcc_n}\}$;
  $account_{pcr}, \{account_{pcc_1} ..., account_{pcc_n}\}$;
  $C, \sigma, \{\pi_{pcc_1}, \pi_{pcc_2},..., \pi_{pcc_n}\}$;
  $\{deposit_{pcc_1}, deposit_{pcc_2},..., deposit_{pcc_n}\}$   $trequest,$
  $deposit_{pcr}, t_{pcp}, creation\_time\ close\_time$;
public Create()
    Input: $Req^{pcr \rightarrow bs_j}$;
$Contract\_address \leftarrow H(ts \mid\mid K_{pcr})$ ;
$ID_{pcr} \leftarrow K_{pcr}$ ; $account_{pcr} \leftarrow addr_{pcr}$;
$deposit_{pcr} \leftarrow$ Move($balance_{pcr}, c$);
$C \leftarrow c$ ; $\sigma \leftarrow c$ ; $trequest \leftarrow ts$ ;
$Rep_{pcr} \leftarrow (Rep_{pcr}$ - 1) ; $Consensus()$ ;
private Negotiate()
    Input: { $Mes^{v_1 \rightarrow bs_j}$,..., $Mes^{vm \rightarrow bs_j}$ } ;
    $\{v_1,..., v_l\} \leftarrow$ Match($\{loc_{v_1},... , loc_{v_m}\}, loc_{pcr}, size_{cz}$)
      ;
    $\{\pi_{v_1},...,\pi_{v_l}\} \leftarrow$ formula (15);
    $\forall\ v_i \in \{v_1,..., v_l\}$ : Send ($Mes^{bs_j \rightarrow v_i}(\pi_{v_i},\sigma)$) ;
private Deploy()
    Input: $\{Resp_{msg}^{v_1 \rightarrow bs_j},..., Resp_{msg}^{v_l \rightarrow bs_j}\}$ ;
    $\{pcc_1,..., pcc_{n'}\}, \{v_1,..., v_{l-n'}\} \leftarrow$ Analyze
      ($\{Resp_{msg}^{v_1 \rightarrow bs_j},..., Resp_{msg}^{v_l \rightarrow bs_j}\}$);
    for $v_i \in \{pcc_1,..., pcc_{n'}\}$ do
        if ($balance_{v_i} > 0$) then
            $ID_{pcc_i} \leftarrow K_{v_i}$ ; $account_{pcc_i} \leftarrow addr_{v_i}$;
            $\pi_{pcc_i} \leftarrow$ formula (15);
            if ($balance_{v_i} >= \sigma$ ) then
                $deposit_{pcc_i} \leftarrow$ Move($balance_{pcc_i}, \sigma$);
                $Rep_{v_i} \leftarrow (Rep_{v_i} + 1)$;
            else
                $deposit_{pcc_i} \leftarrow$ Move($balance_{pcc_i}$);
                $Rep_{v_i} \leftarrow (Rep_{v_i} + 0.5)$;
            end
        end
    end
    $\forall\ v_i \in \{v_1,..., v_{l-n'}\}$: $Rep_{v_i} \leftarrow (Rep_{v_i}$ - 1);
    if Consensus()==true then
        $creation\_time \leftarrow timestamp$ ; set($t_{pcp}$);
        Send ($Conf^{b_j \rightarrow pcr}(t_{pcc})$);
        $\forall\ v_i \in \{pcc_1,..., pcc_n\}$:
          Send ($Conf^{b_j \rightarrow v_i}(t_{pcc})$);
    end
private Invoke()
    Input: $Fb^{pcr \rightarrow bs_j}, \{Fb^{pcc_1 \rightarrow bs_j},..., Fb^{pcc_n \rightarrow bs_j}\}$ ;
    $Execute\_contract()$ ; $Close()$;
private close()
    $close\_time \leftarrow timestamp$ ; $Consensus()$;
```

Figure 22: Cooperative Pseudonym Changing Smart Contract

B. Negotiate

After creating the SC, a set of PCCs should be selected to participate with the PCR in the next PCP. For this reason, each bsj keeps monitoring vehicles under its coverage. Since the privacy level is not part of the standard structure of the beacon, each vehicle (vi) then periodically broadcasts a message to bsj: $Mes^{vi\rightarrow bsj}$ = EPK_{bsj} (loc_{vi} ||pv_{vi} ||K_{vi}|| Sig_{Kvi} || $Cert_{Kvi}$ ||ts). This message is encrypted by PK_{bsj} and includes the current position of the vehicle (loc_vi)and its privacy level (pv_{vi}). It also includes vi's current pseudonym (K_{vi}), the corresponding signature (Sig_{Kvi}), certificate ($Cert_{Kvi}$), and timestamp (ts). This message should be encrypted since the privacy level is private information. Sharing this information can have social impacts on drivers.

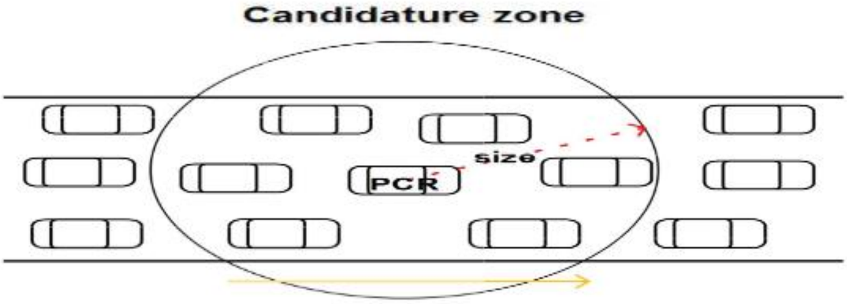


Figure 23: Candidature zone for a given PCR

In step (20), once a PCR's request is received by bsj, it matches between the received request and the monitoring (m) vehicles to select the l vehicles {v1,...,vl} from the candidature zone of the PCR. As illustrated in Figure 23, the Candidature Zone (CZ) is defined as the road area that contains the potential candidate vehicles that can cooperate with the PCR in its PCP. More specifically, CZ is a circle whose centre is the position of the vehicle and its radius is the size of CZ, denoted as sizeCZ. After selecting the potential cooperative candidates, bsj calculates the number of coins to pay for each candidate vehicle {πv1,...,πvl}. The need to participate in the PCP is different from a vehicle to another according to its current privacy level. In addition, the reputation value of a vehicle is a good indicator of the level of cooperation of vehicles. To this end, we adopt the payment of cooperative vehicles according to their privacy levels and their reputation values. In other words, vehicles with high privacy levels and reputation values will be paid more for rewarding them for their cooperative behavior and for their sacrifices since their need to change their pseudonyms is weak compared to other vehicles. In step (21), the payments of vehicles are calculated according to their privacy levels and reputation values using the following formula (19):

$$\pi_{v_i} = \frac{rep_{v_i} * pv_{v_i}}{\sum_{j=1}^{l}(rep_{v_j} * pv_{v_j})} * C$$

Formula 19

In step (22), once of the calculation of the payments of cooperative vehicles is done, bsj sends a message for each selected vehicle:$Mes^{bsj\rightarrow vi}$= EK_{vi} (π_{vi} || σ || Sig_{PKbsj} ||ts). This message is encrypted by the current vehicle's pseudonym (K_{vi}) and includes the number of coins (π_{vi}), which the vehicle will receive in case of cooperation, the penalty price (σ) applied to the vehicle in case of no respect of SC's clauses, and the signature (Sig_{PKbsj}) and the timestamp ts.

C. Deploy

Before deploying the SC into the consortium blockchain, bsj needs to wait for responses from candidates vehicles to check their willingness to participate in the PCP: $Resp_{msg}{}^{vi\rightarrow bsj}$= EPK_{bsj}($resp_{vi}$ || $addr_{vi}$|| K_{vi} || $Sig_{Kv\ i}$|| $Cert_{Kvi}$ || ts). These responses are encrypted by PK_{bsj} and include the cooperation decision of the candidate vehicle($resp_{vi}$), (vi)'account address ($addr_{vi}$), vi's current pseudonym (K_{vi}), the corresponding signature (Sig_{Kvi}), certificate ($Cert_{Kvi}$),and timestamp (ts).

In step (26), the response messages are analyzed to distinguish between cooperative vehicles and non-cooperative vehicles. The balance of each cooperative vehicle is checked in step (28). If the balance is positive, the vehicle assigned as an PCC and its related parameters (ID_{pcci}, $account_{pcci}$) are initialized in step (29). In step (30), a recalculation of the vehicle's payment using the formula 1 is also necessary since the number of selected l vehicles may differ from the number of cooperative vehicles. In addition, in step (31), bj checks if the vehicle has enough coins to pay for the penalty σ (if applicable). If the check passes, then a deposit of σ coins is moved from the vehicle's balance to the contract address instep (32) and the vehicle's reputation is increased by 1 in step (33). Otherwise, existing coins in the vehicle's balance are moved to the contract address in step (35) but the vehicle's reputation is increased by only 0.5 in step (35). On the other hand, the reputations values of all non-cooperative vehicles (l−n') will be decreased by 1 in step (40). In this stage, the SC is ready to be deployed into the blockchain. After reaching consensus in the consortium blockchain, the SC is successfully deployed and can be accessed by all the blockchain nodes. Once the contract is deployed, bsj sets creationtime and tpcp in step (42). Then,it sends a confirmation message to the PCR : $Conf^{bsj-\rightarrow pcr}$=$EK_{pcri}$(Contract_address || tpcp || Sig_{Kbsj} || ts) in step (43). A confirmation is also sent to each PCC {pcc_1,...,pcc_n} in step (44) :$Conf^{bsj-\rightarrow pcci}$=$EK_{pcci}$(Contract_address || tpcp || π_{pcci} || Sig_{PKbsj} || ts).The confirmations message include the contract address (Contractaddress), (tpcp), the signature Sig_{PKbsj} and the timestamp ts. In addition, $Conf^{bsj-\rightarrow pcci}$ includes the amount of coins should each PCC gets after having participated in the PCP.

D. Invoke

This function is automatically called by bsj as soon as (t >=tpcp) to perform necessary transactions and financial settlements. This function needs an input from the PCR and each PCC to verify whether PCP is executed according to the SC clauses. Necessary penalties followed by decreasing reputation values are also applied to malicious PCCs. Specifically, PCR sends a feedback message to bsj: $Fb^{pcr-\rightarrow bsj}$=EPK_{bsj}(Contract_address || {pcc_1,...,pcc_n}|| K_{pcr} || Sig_{Kpcr}|| $Cert_{Kpcr}$|| ts). This message is encrypted by PK_{bsj} and includes the contract address (Contract_address), the pseudonyms of vehicles that change their pseudonyms in the PCR's PCP. This message also includes PCR's current pseudonym (Kpcr), the corresponding signature (Sig_{Kpcr}), certificate (CertKpcr), and a timestamp (ts). Each PCC should also send a feedback message to bsj to confirm its participation in the PCP: $Fb^{pcci-\rightarrow bsj}$=EP K_{bsj} (Contractaddress ||K_{pcci}|| K'pcci||Sig_{Kpcci}|| $Cert_{Kpcci}$ || ts). This message is also encrypted (PK_{bsj}) and includes the contract address (Contract_address), the PCR's current pseudonym (Kpcci), the PCR's previous pseudonym (K'pcci), the corresponding signature Sig_{Kpcci}, certificate $Cert_{Kpcci}$, and timestamp ts. Once bsj receives these confirmation messages, it executes the SC is in step (49). Thus, the financial transactions concerning payments and penalties are generated and prepared for block building. Finally, the function Close() is called for running the consensus progress and closing the smart contact.

E. Close

This function starts by deactivating all the functions of the SC and assigning the close time (closetime). Then, a consensus process is executed in step (52) to update the ledger, as described in section 3.4.4.4.

3.4.4.3 Smart Contract Optimization

In this section, we propose an optimization for the pseudonym cooperation SC. The goals of this optimization are to (i) minimize the number of smart contracts managed by the scheme, (ii) reduce the price paid by PCRs, and (iii) increase the location privacy levels obtained in PCPs. To implement the SC optimization process, during ΔT1, bsj collects requests for PCRs. At the end of this period, bsj runs a k-means algorithm to group PCRs into clusters according to their positions and their directions (A. Rodriguez et al.). PCRs within the same cluster will participate in the same PCP. In the following, we denote the SC described in the previous section as the Standard SC (SSC). The Optimized SC (OSC) is derived from the SSC and its implementation is given in Figure 25. Unlike the SSC, which is one-to-many SC between one PCR and multiple PCCs, the OSC is a many-to-many SC between multiple PCRs and multiple PCRs. Thus, in the OSC, the state variables ID_{pcr}, $account_{pcr}$, $deposit_{pcr}$ are replaced by $\{ID_{pcr0},...,ID_{pcrn}\}$, $\{account_{pcr0},...,account_{pcrn}\}$, $\{deposit_{pcr0},...,deposit_{pcrn}\}$ respectively. The OSC contains the same functions as the SSC, but all of them are private. In the following, we present the main optimizations in these functions:

A. Create

Unlike the SSC, the function creates turns to private in the OSC. As aforementioned, an OSC is created for each cluster of PCRs. The create function then takes the group of requests belonging to the same cluster as an input. For each request $Req^{pcri\text{–}\rightarrow bsj}$(ci), bsj checks if the vehicle has a positive reputation and enough coins to pay for the PCP. If this condition is satisfied, the vehicle will be assigned as a pcri and its related state variables (ID_{pcri}, $account_{pcri}$) will be initialized in steps (9) and (10) respectively. In addition, in step (11), a number of coins (ci) is moved from the PCR's balance to the contract address as a deposit ($desposit_{pcri}$), and, in step (12), trequest is initialized. However, in the case of the vehicle's balance is less than ci, its reputation value is decreased in step (15). Thus, a consensus process is necessary later in step (18) to keep the values of reputation updated in the ledger. Furthermore, in step (19), the contract address is initialized to the hash of the concatenated pseudonyms of PCRs and the timestamp. Also, in step (20), the total number of coins to pay (costs) for the PCP is initialized by the average number of coins offered by PCRs, which is calculated using formula 20:

$$C = \frac{1}{n}\sum_{j=1}^{n} c_j$$

Formula 20

Since the reputation values of PCRs are different, we propose to adapt the contribution of each PCR in the total costs (C) according to its reputation in step 21. In other words, PCRs with high reputation values will pay less more than other vehicles. The contribution of each PCR is computing using formula 21:

$$contrib_i = \frac{C}{Rep_{pcr_i} * \sum_{j=1}^{n} \frac{1}{Rep_{pcr_j}}}$$

Formula 21

B. Negotiate

In step 26, unlike the SSC, the OSC matches between the positions of monitoring vehicles and PCRs' positions of the same cluster to select the candidate vehicles. Therefore, as shown in Figure 24, the CZ of the OSC is the union of CZs of these PCRs.

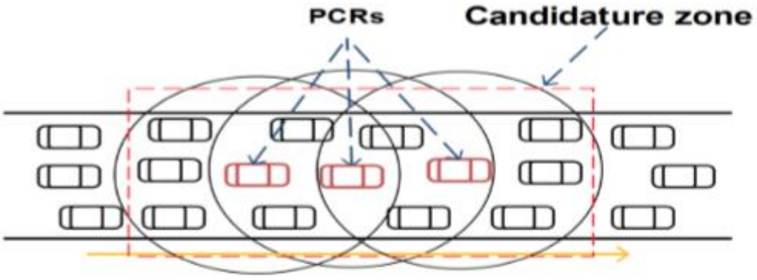


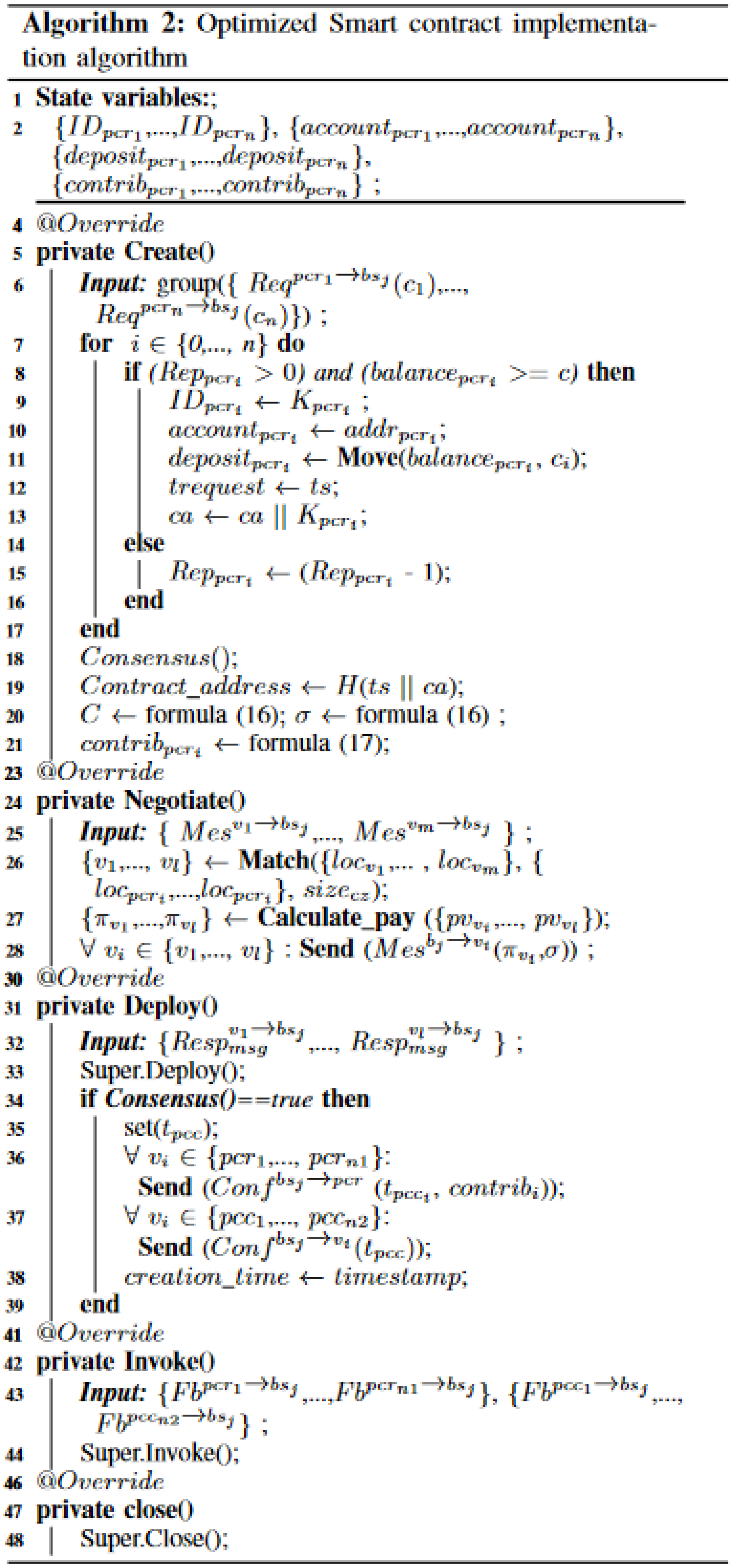
Figure 24: Candidature zone for the optimized smart contract

C. Deploy

The OSC executes the same code as the SSC. Except, in step36, once the contract is deployed, bsj sends a confirmation to each PCR specifying the contract address, tpcc and its contribution to the total costs of the PCP ($contrib_{pcr}$), which is calculated using the formula17.

D. Invoke

Compared to the SSC, the OSC takes feedback for each PCR participating in the PCP.



```
Algorithm 2: Optimized Smart contract implementation algorithm
State variables:;
  $\{ID_{pcr_1},...,ID_{pcr_n}\}$, $\{account_{pcr_1},...,account_{pcr_n}\}$,
  $\{deposit_{pcr_1},...,deposit_{pcr_n}\}$,
  $\{contrib_{pcr_1},...,contrib_{pcr_n}\}$ ;
@Override
private Create()
    Input: group({ $Req^{pcr_1 \rightarrow bs_j}(c_1)$,...,
      $Req^{pcr_n \rightarrow bs_j}(c_n)$}) ;
    for $i \in \{0,..., n\}$ do
        if ($Rep_{pcr_i} > 0$) and ($balance_{pcr_i} >= c$) then
            $ID_{pcr_i} \leftarrow K_{pcr_i}$ ;
            $account_{pcr_i} \leftarrow addr_{pcr_i}$;
            $deposit_{pcr_i} \leftarrow$ Move($balance_{pcr_i}$, $c_i$);
            $trequest \leftarrow ts$;
            $ca \leftarrow ca \mid\mid K_{pcr_i}$;
        else
            $Rep_{pcr_i} \leftarrow (Rep_{pcr_i}$ - 1);
        end
    end
    $Consensus()$;
    $Contract\_address \leftarrow H(ts \mid\mid ca)$;
    $C \leftarrow$ formula (16); $\sigma \leftarrow$ formula (16) ;
    $contrib_{pcr_i} \leftarrow$ formula (17);
@Override
private Negotiate()
    Input: { $Mes^{v_1 \rightarrow bs_j}$,..., $Mes^{v_m \rightarrow bs_j}$ } ;
    $\{v_1,..., v_l\} \leftarrow$ Match($\{loc_{v_1},... , loc_{v_m}\}$, {
      $loc_{pcr_i},...,loc_{pcr_i}\}$, $size_{cz}$);
    $\{\pi_{v_1},...,\pi_{v_l}\} \leftarrow$ Calculate_pay ($\{pv_{v_i},..., pv_{v_l}\}$);
    $\forall\ v_i \in \{v_1,..., v_l\}$ : Send ($Mes^{b_j \rightarrow v_i}(\pi_{v_i},\sigma)$) ;
@Override
private Deploy()
    Input: $\{Resp_{msg}^{v_1 \rightarrow bs_j}$,..., $Resp_{msg}^{v_l \rightarrow bs_j}$ } ;
    Super.Deploy();
    if Consensus()==true then
        set($t_{pcc}$);
        $\forall\ v_i \in \{pcr_1,..., pcr_{n1}\}$:
          Send ($Conf^{bs_j \rightarrow pcr}$ ($t_{pcc_i}$, $contrib_i$));
        $\forall\ v_i \in \{pcc_1,..., pcc_{n2}\}$:
          Send ($Conf^{bs_j \rightarrow v_i}(t_{pcc})$);
        $creation\_time \leftarrow timestamp$;
    end
@Override
private Invoke()
    Input: $\{Fb^{pcr_1 \rightarrow bs_j}$,...,$Fb^{pcr_{n1} \rightarrow bs_j}\}$, $\{Fb^{pcc_1 \rightarrow bs_j}$,...,
      $Fb^{pcc_{n2} \rightarrow bs_j}\}$ ;
    Super.Invoke();
@Override
private close()
    Super.Close();
```

Figure 25: Optimized Smart contract implementation algorithm

E. Close

No change is done in this function compared to the SSC.

3.4.4.4 Utility-based Delegated Byzantine Fault Tolerance Consensus Protocol

Consensus processes should be carried to ensure that each member of the consortium blockchain has a coherent and recognized of the whole ledger. To efficiently reach the consensus in our scheme, we propose a Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus protocol, which is based on Castro et al. at “Practical Byzantine fault tolerance”. The consensus protocol comprises two steps:(i) the consensus members and leader selection, and (ii) the consensus process.

A. Consensus members and leader selection

The members of the consortium blockchain (BSs) have two types of roles: simple members and consensus members. While a consensus member can participate in consensus processes, a simple member can only broadcast transactions into the blockchain network and accept the validated blocks. The selection of the consensus members is done according to their utility values {U_{bs1}, U_{bs2}, ..., U_{bs3}, ...U_{bsn}}, which are calculated on the basis scores received from vehicles. As shown in formula 22, the top (Ω) BSs with the highest utility values are selected as consensus members. The set of consensus members is denoted asΩ={1,...,Ω}. We assume that Ω>= 3f+1, where f is the maximum number of malicious members in the consortium blockchain.

$$\{bs_1, ...bs_\Omega\} = Max(\{U_{bs_1}, U_{bs_2}, ..., U_{bs_3}, ...U_{bs_n}\}, \Omega)$$

Formula 22

As shown in formula 23, U_{bsk}, the utility of a bsk is the average of the sum of scores calculated by PCR(s) and PCCs weighted by their reputation values. It is worth mentioning that depending on a PCP, a vehicle can be either a PCR or a PCC. In addition, during their journey on the road, vehicles can participate in several PCPs. Thus, before being out of the coverage of bsk, each vehicle sends its scoring values to bsj.

$$U_{bs_k} = \frac{1}{nb_{sco_{pcr}}} * \sum_{i=1}^{nb_{sco_{pcr}}} (Rep_{pcr_i} * Score_{pcr_i}) + \frac{1}{nb_{sco_{pcc}}} * \sum_{j=1}^{nb_{sco_{pcc}}} (Rep_{pcc_j} * Score_{pcc_j})$$

Formula 23

nb_{scopcr} and nb_{scopcc} are the numbers of scores received from PCRs and PCCs, respectively. $Score_{pcri}$ is the score given by a pcri to bsk, which is calculated using formula 24. In this formula, $_{nb1pcp}$ is the number of PCPs where the vehicle is involved as a PCR. The score of a bsk is calculated based on the average of the sum of values obtained in each executed PCP. These values are the value to money (vm) given by the formula 26, which assesses the monetary cost against the location privacy obtained after executing a PCP, the processing speed (ps) given by the formula 27, which assesses the speed of establishing the SC, and the consensus speed of the block (cs), given by the formula 28.

$$Score_{pcr} = \frac{\sum_{i=1}^{nb1_{pcp}} (vm_i + cs_i + ps_i)}{nb_{pcp}}$$

Formula 24

On the other hand, Score$_{pcc}$ is the score given by a pcci to bsk. As shown in the formula 11, a pcc calculates the score according to the average of the sum of cs (formula 23) and ps (formula 24) values obtained after each PCP. Here, nb2$_{pcp}$ is the number of PCPs where the vehicle is involved as a PCC. Moreover, this score also takes into account the number of PCPs' proposals (nb$_{prop}$) received from the bsk.

$$Score_{pcc} = \frac{\sum_{i=1}^{nb_{pcp}} (cs_i + ps_i)}{nb_{pcp}} + nb_{prop}$$

Formula 25

As aforementioned, vm is a metric to assess the monetary cost against the location privacy level obtained executing a PCP. vm is calculated using formula 26, where priv is the obtained location privacy level, and pric is the price paid for a given PCP.

$$vm = \frac{priv}{pric}$$

Formula 26

ps is a metric to assess the effort taken by a bs to establish a SC, which includes the selection of the candidate vehicles and sending/receiving messages. ps is calculated using formula 27, where tp is the effective processing time, and max$_{tp}$ is the maximum expected time for processing.

$$ps = \frac{max_{tp} - tp}{max_{tp}}$$

Formula 27

cs is the consensus speed, which is a metric defined to measure how faster the consensus process was done from the block production to the block insertion in the consortium blockchain. cs is calculated using formula 28, where tc is the effective time for the consensus process and max$_{tc}$ is the maximum taken for the consensus process of one block.

$$cs = \frac{max_{tc} - tc}{max_{tc}}$$

Formula 28

A network operator who manages a set of BSs aims that their BSs are part of the set of the consensus members to receive coins for each performed consensus process. Thus, BSs will do their best to increase their utility values for participating in the consensus process. However, BSs will try to tamper the score values of vehicles for increasing their utility and the reby monopolizing the consensus process. For this reason, we also propose to store the utility values into the ledger. The scores of vehicles are broadcast to the blockchain. Each ΔT2, the utility values of BSs are calculated, and a consensus process is carried out to update the set of the consensus members (Ω).

In our scheme, the first leader is the member with the highest utility value. After that, the leader pis changed after each consensus process or if it fails during the current consensus process. The selection of the next leader pis done according to a round-robin (circular) policy using formula 29:

$$p = v \ mod \ \Omega$$

Formula 29

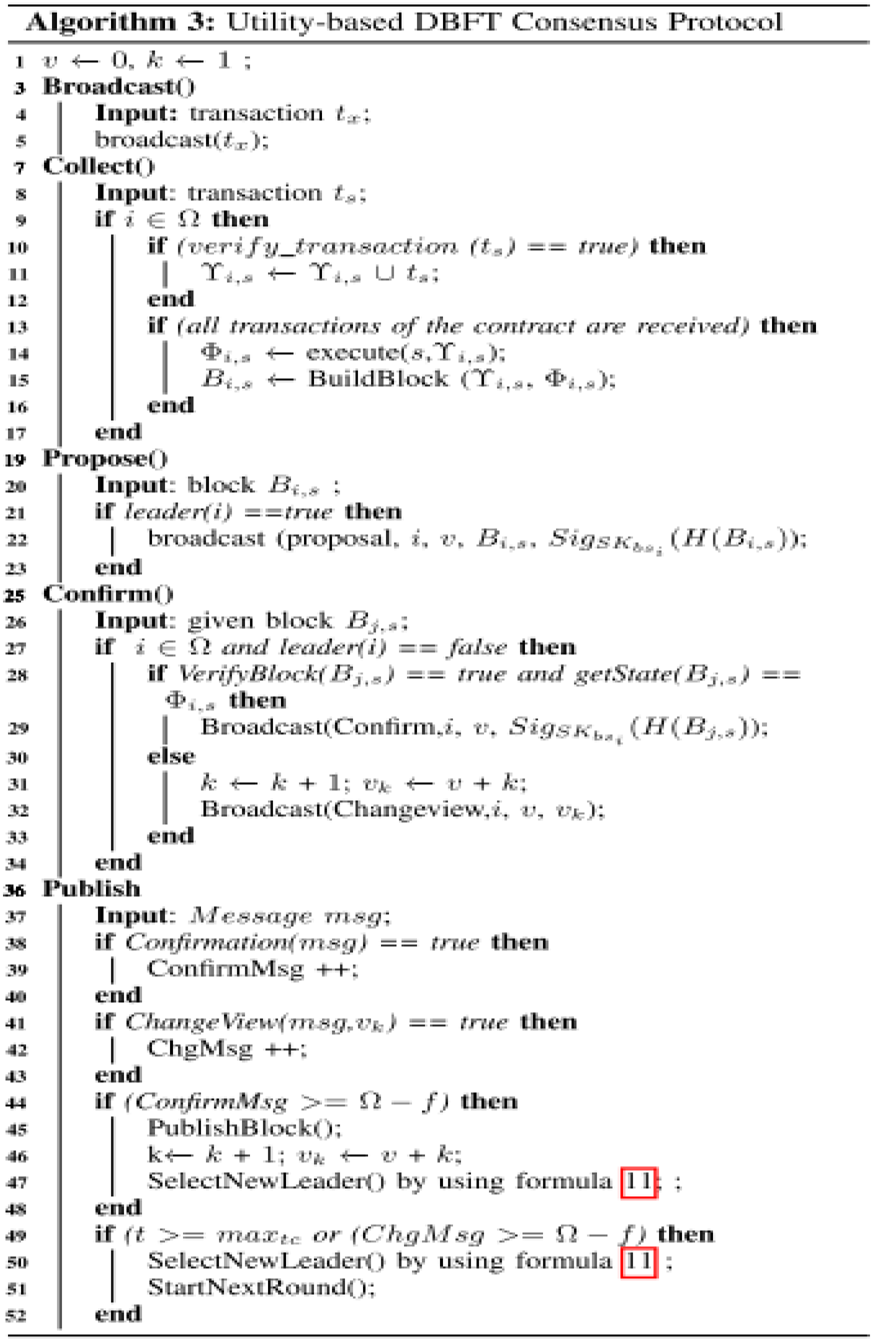
In Ω, the consensus members are in descending order according to their utility values starting from index 0. Based on Castro et al. at “Practical Byzantine fault tolerance” a view is a period of time in which a given consortium member is the leader. In formula 29, v is an identifier of a given period of time. Therefore, a view change means switching to a different leader.

B. Consensus process

The consensus process runs by a consensus member (i) is described in Figure 26. This algorithm describes the consensus process applied to the blocks (the transactions and states) related to a (SC). However, the same consensus process is applied to the blocks related to the reputation and utility values. Here tsi is a transaction record related to the SC, $Y_{i,s}$ is a set of SC’s transactions validated by the consensus member i. $\Phi_{i,s}$ is the updated state after the execution of SC with the set of corresponded transactions $Y_{s.Bi}$ is a local block created by the consensus member i, verifytransaction (ts) is a function to verify the validity of a transaction ts, execute ($Y_{i,s}$) is a function that locally executes the SC with the corresponded transactions $Y_{i,s}$, BuildBlock($Y_{i,s}$,$\Phi_{i,s}$) is to build local block with the transaction set $Y_{i,s}$ and the state set $\Phi_{i,s}$. The consensus process then contains the following steps:

1. *Broadcast*: When an SC is triggered between PCR(s) and PCCs under the coverage of bsj, this latter broadcasts all the corresponded transactions into the whole consortium blockchain for audit and verification.
2. *Collect*: All consensus members collect all SC’s transactions. Each transaction ts is verified in step (10) and only the validated transactions are added to the list of validated transactions $Y_{i,s}$ in step (11). Each consensus member waits to receive all the SC’s transactions before it locally executes the SC in step (14). The changed states after executing the SC are saved in the local state ledger of each consensus member. All validated transactions and states are ordered by the timestamp and packaged into a block in step (15). Building a local block by each consensus member significantly reduces the time of verifying candidate blocks. Indeed, a no-leader consensus member can verify a candidate block received from the leader by simply comparing its local block with the candidate block.
3. *Propose*: After all non-leader consensus members have finished building their local blocks, the leader consensus member broadcasts a proposal to all non-leader consensus members in step (22). This proposal includes the leader’s identifier (i), the view v, the local block ($B_{i,s}$), and the hash value of the block (H($B_{i,s}$)) singed by SK_{bsi}.
4. *Confirm*: Once a non-leader vehicle receives a candidate block Bj,s, it first verifies its validity using verifyBlock(), then it uses the function getState() to retrieve the state of the block for comparing it with its local state Φi,s. If these checks passed, each non-leader consensus member broadcasts a confirmation message in step (29), which includes its identifier i, the view change v and the signature the hash of the block(Sig_{SKbs}i(H(Bj,s)). However, if the received block is not valid, the view change will be triggered, where the next view change vk is calculated in step (31). Therefore, the non-leader consensus member will broadcast the changeviewMsg message in step (32), which includes non-leader’s identifier(i), the current view v, and the changed view vk.
5. *Publish*: Each consensus member keeps counting the number of received confirmations and

the number of views changes vk in steps (39) and (42), respectively. If the number of received confirmation messages is no less (ω−f) massages from other distinct consensus members, the consensus is reached, and the block is ready to be published in the blockchain. To ensure tractability and verification, each block is added in chronological order into the blockchain and includes a cryptographic hash to the prior block. To prepare for the next consensus process, the view is changed in step (46) and the next leader is selected in step (47) using the formula 29. However, if the max period to reach the consensus (max_{tc}) has passed or the number of received view change messages with the same vk is at least (Ω−f) from distinct consensus members, a new leader is selected in step (50) and the next round of the consensus process will start in step (51).



```
Algorithm 3: Utility-based DBFT Consensus Protocol
$v \leftarrow 0$, $k \leftarrow 1$ ;
Broadcast()
    Input: transaction $t_x$;
    broadcast($t_x$);
Collect()
    Input: transaction $t_s$;
    if $i \in \Omega$ then
        if ($verify\_transaction$ ($t_s$) == $true$) then
            $\Upsilon_{i,s} \leftarrow \Upsilon_{i,s} \cup t_s$;
        end
        if (all transactions of the contract are received) then
            $\Phi_{i,s} \leftarrow$ execute($s$,$\Upsilon_{i,s}$);
            $B_{i,s} \leftarrow$ BuildBlock ($\Upsilon_{i,s}$, $\Phi_{i,s}$);
        end
    end
Propose()
    Input: block $B_{i,s}$ ;
    if leader(i) ==true then
        broadcast (proposal, $i$, $v$, $B_{i,s}$, $Sig_{SK_{bs_i}}(H(B_{i,s}))$;
    end
Confirm()
    Input: given block $B_{j,s}$;
    if $i \in \Omega$ and leader(i) == false then
        if VerifyBlock($B_{j,s}$) == true and getState($B_{j,s}$) ==
          $\Phi_{i,s}$ then
            Broadcast(Confirm,$i$, $v$, $Sig_{SK_{bs_i}}(H(B_{j,s}))$;
        else
            $k \leftarrow k + 1$; $v_k \leftarrow v + k$;
            Broadcast(Changeview,$i$, $v$, $v_k$);
        end
    end
Publish
    Input: $Message\ msg$;
    if Confirmation(msg) == true then
        ConfirmMsg ++;
    end
    if ChangeView(msg,$v_k$) == true then
        ChgMsg ++;
    end
    if (ConfirmMsg >= $\Omega - f$) then
        PublishBlock();
        k$\leftarrow k + 1$; $v_k \leftarrow v + k$;
        SelectNewLeader() by using formula 11; ;
    end
    if ($t >= max_{tc}$ or ($ChgMsg >= \Omega - f$) then
        SelectNewLeader() by using formula 11 ;
        StartNextRound();
    end
```

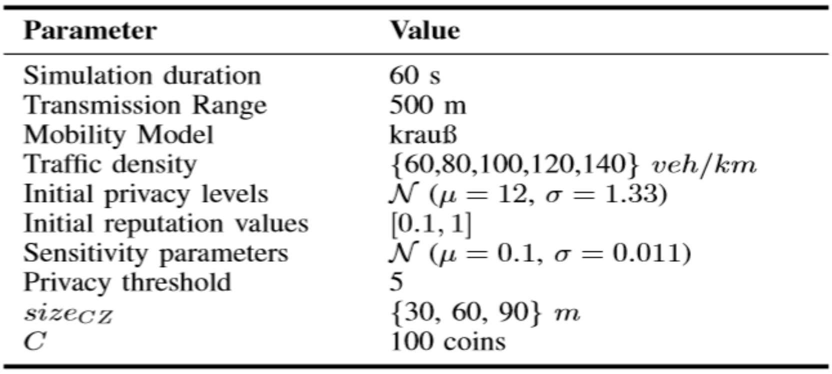
Figure 26: Utility-based DBFT Consensus Protocol

3.4.4.5 Performance evaluation

In this section, we evaluate the performance of the proposed scheme. We first evaluate the cooperative behavior in our scheme. We then perform a monetary analysis on the payments received by PCCs and the costs paid by PCRs considering both SSCs and OSCs. In addition, we evaluate the time needed to reach the consensus in the consortium blockchain and carry out an analytic evaluation of the utility function used to select the first leader in the set of the consensus members. Finally, we formulate a security game to capture different attacker behaviors in our scheme.

A. Cooperative behaviour

We have carried out a set of simulations to evaluate the cooperative behavior of vehicles in our scheme. We first study the average number of cooperative vehicles inside PCPs in our scheme compared to random and basic cooperation strategies. We then evaluate the impact of variating both traffic density (ρ) and the size of the candidature zone (sizeCZ) on the average number of cooperative vehicles inside PCPs and the number of performed PCPs respectively. Finally, we compare the number of created SCs and the average number of vehicles per SC considering both SSCs and OSCs.



Parameter	Value
Simulation duration	60 s
Transmission Range	500 m
Mobility Model	krauß
Traffic density	$\{60,80,100,120,140\}$ veh/km
Initial privacy levels	$\mathcal{N}$ $(\mu = 12,\ \sigma = 1.33)$
Initial reputation values	$[0.1, 1]$
Sensitivity parameters	$\mathcal{N}$ $(\mu = 0.1,\ \sigma = 0.011)$
Privacy threshold	5
$size_{CZ}$	$\{30,\ 60,\ 90\}$ m
C	100 coins

Table 16: Simulation Parameters

These simulations are conducted using Veins simulation Framework (C. Sommer et al. 2011). We considered the case of a freeway road. We simulated a 3-lane straight road section of 3 Km. The mobility of vehicles is generated using SUMO and follows the Krauß mobility model. As shown in Table 16, we consider that traffic density is ranging from 60 to 140 vehicles/km. The initial reputation values of vehicles are randomly initialized with values ∈ [0.1,1]. The privacy level values of vehicles are initialized according to a normal distribution N(μ= 12,σ= 1.33). To capture the location privacy level as a function of the power of the adversary, we adopt the user-centric model proposed in "Non-cooperative location privacy" by Freudiger et al. The loss of location privacy of vehicles is modelled using a linear function, where the privacy loss increases with time according to a sensitivity parameter, 0< λi<1. This maximum value of privacy loss is the location privacy protection level achieved at the last PCP. The loss of privacy is set to 0 after each PCP. In our simulations, we consider that sensitivity values of vehicles are initialized according to a normal distribution N(μ= 0.1,σ= 0.011). Vehicles look to perform PCPs when their privacy levels are close to the privacy threshold, which is set to 5. We also consider different values of sizeCZ. We run simulation several times to calculate the average value of 95% confidence interval. Figure 27 compares the average number of cooperative vehicles inside PCPs in our scheme with two cooperative strategies: random and basic. The random strategy represents naive cooperative behaviour, where vehicles take the cooperation decision without considering their self-interests. In the basic cooperative strategy, vehicles participate in the PCP only if their privacy levels go below the privacy threshold. The results show that the average number of cooperative vehicles in our scheme is higher than the random and basic strategies, whatever the traffic density is.

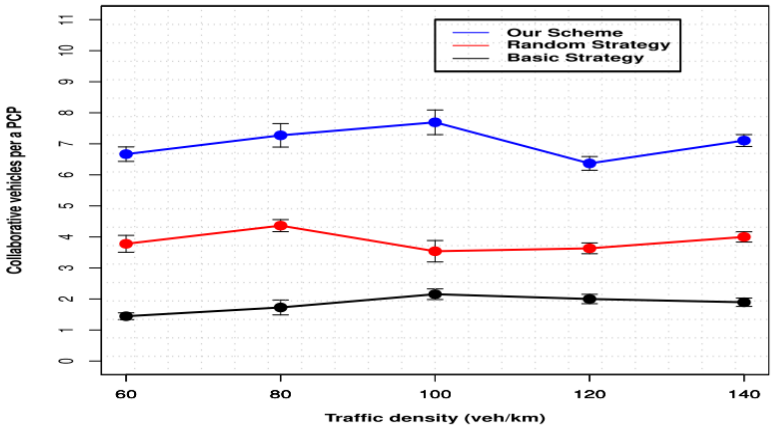


Figure 27: The average number of cooperative vehicles per PCPas a function of traffic density comparing our scheme with two cooperation strategies (sizeCZ= 60m)

In Figure 28, we evaluate the impact of variating the size CZ on the average number of cooperative vehicles per PCP over different traffic densities. Our results show that the number of cooperative vehicles increases with size CZ. However, numbers remain stable over different traffic density levels. This is mainly due to the predefined parameters of the mobility model, such as the safety distance and changing lane strategies, which prevents having more vehicles in CZs when the traffic density increases. This leads to an increase in the number of performed PCPs with the increase of the traffic density, as we can see in Figure 29. Indeed, the smaller the CZs, the faster the number of the performed PCPs increases with the traffic density.

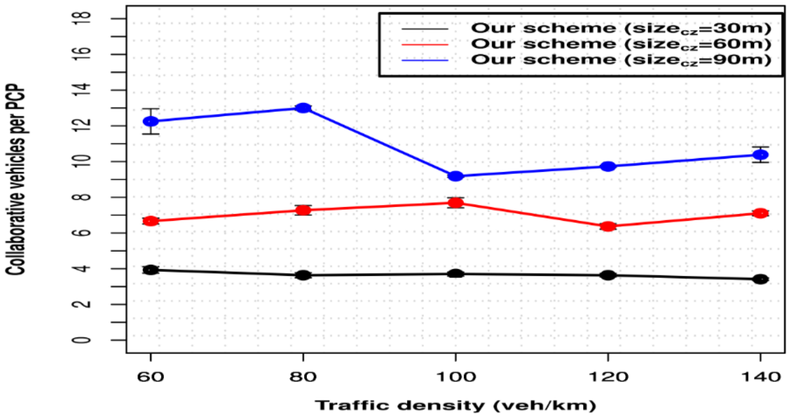


Figure 28: The average number of cooperative vehicles per PCP as a function of traffic density variating sizeCZ

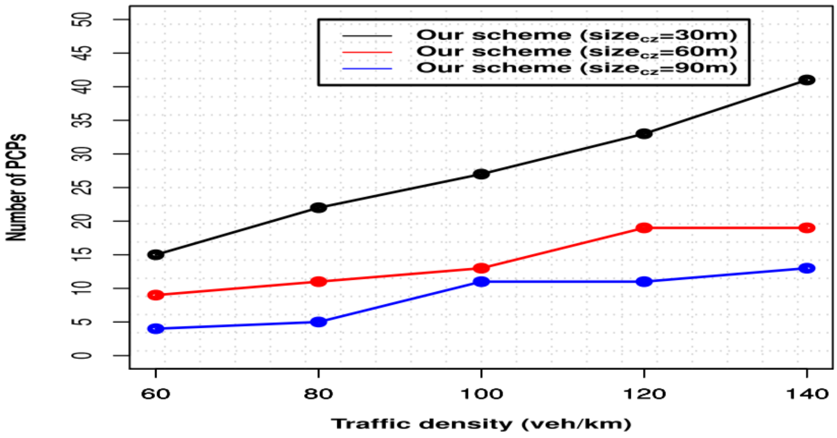


Figure 29: The number of performed PCPs as a function of traffic density variating sizeCZ

In our previous evaluations, we consider that PCPs only run under SSCs. In the following evaluation, we compare two scenarios: (i) PCPs running under SSCs, and (ii) PCPs running under OSCs. The scikit-learn python library (https://scikit-learn.org) is used to run k-means clustering with k = 4 to create groups of PCRs associated with OSCs. Figure 30 (a) shows the number of PCRs per each OSC. Figure 30 (b) compares the number of SCs created in each scenario. The results show that using OSCs, our scheme can save more than 65% of the total number of SCs. In addition, Figure 30 (c) shows that the average number of cooperative vehicles inside PCPs is higher when using OSCs. These results confirm that OSCs allows reducing the number of SCs managed by the scheme and increase the privacy level obtained in PCPs.

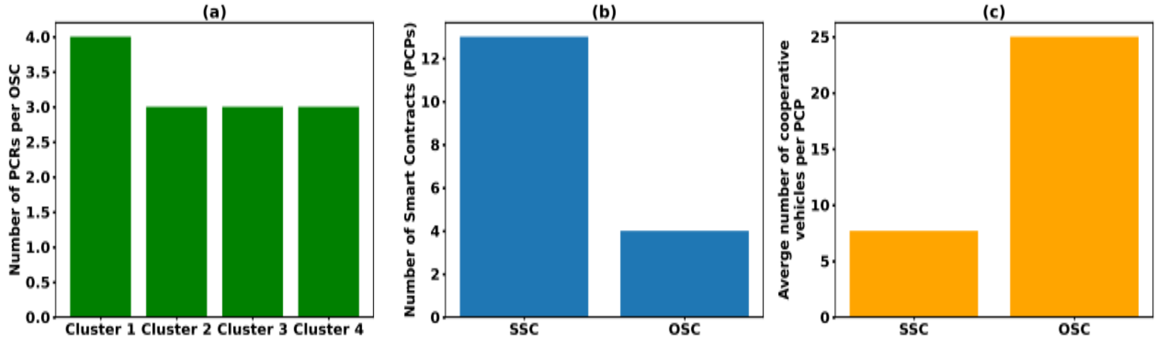


Figure 30: Comparison between PCPs running under SSCs and PCPs running under OSCs. (a) The distribution of PCRs over clusters; (b) The number of generated smart contracts; (c) The average number of cooperative vehicles per PCP; (ρ= 100veh/km and sizeCZ= 60m)

B. Monetary analysis

In this section, we perform a monetary analysis of payments received by PCPs and the cost paid by PCRs under SSCs and OSCs. Figure 31 shows the payments received by five PCCs in three different PCPs.

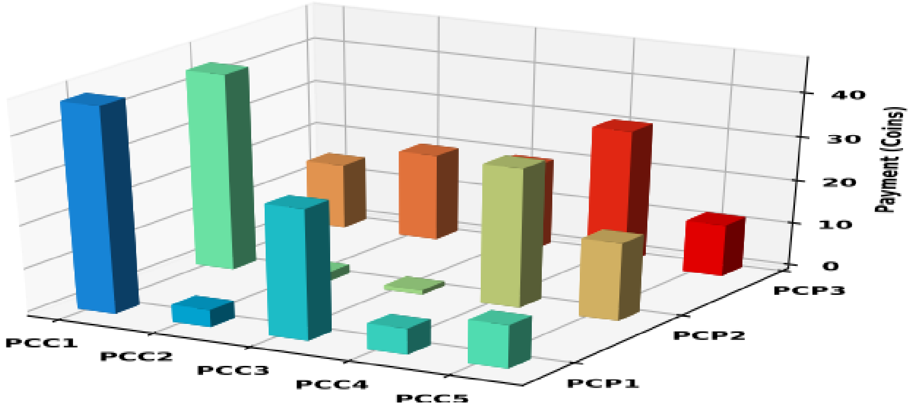
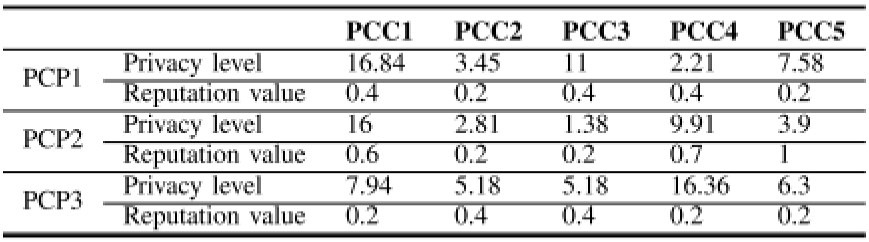


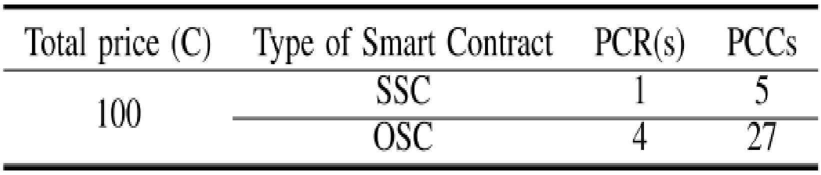
Figure 31: The payment of five vehicles in three different PCPs (ρ= 100veh/km, sizeCZ= 60m, C= 100 coins)



		PCC1	PCC2	PCC3	PCC4	PCC5
PCP1	Privacy level	16.84	3.45	11	2.21	7.58
	Reputation value	0.4	0.2	0.4	0.4	0.2
PCP2	Privacy level	16	2.81	1.38	9.91	3.9
	Reputation value	0.6	0.2	0.2	0.7	1
PCP3	Privacy level	7.94	5.18	5.18	16.36	6.3
	Reputation value	0.2	0.4	0.4	0.2	0.2

Table 17: The privacy levels and reputation values of five vehicles in three different PCPs

These payments are calculated using formula 19 based on the privacy levels and reputation values given in Table 17. As we can see, higher payments are given to vehicles with high reputation values and high privacy levels. Thus, to increase their payments, vehicles always try to increase their reputation values and participate in PCPs even if their privacy levels are high. Figure 12 compares the average payment and privacy level received by PCCs and the cost paid by a PCR under both SSCs and OSCs. As shown in Table 18, if a PCR performs a PCP under an SSC, only five PCCs will cooperate with it. However, if the same PCR performs a PCP under OSC, three other PCRs and 27 PCCs will participate in this PCP. Figure 12 (a) compares the average payment received by a PCC both under an SSC and an OSC. As we can see, the average payment received by a PCC is higher under an SSC than under an OSC. However, as shown in Figure 12 (b), the privacy level obtained by a PCC under an OSC is higher than the obtained under an SSC. Figure 12 (c) compares the price paid by one PCR (PCR3) under both an SSC and an OSC. As we see, the price paid by PCR3 under an OSC is more 80% lower than the price paid under an OSC.



Total price (C)	Type of Smart Contract	PCR(s)	PCCs
100	SSC	1	5
	OSC	4	27

Table 18: Comparison of the number of PCR(s) and PCCs under an SSC and an OSC

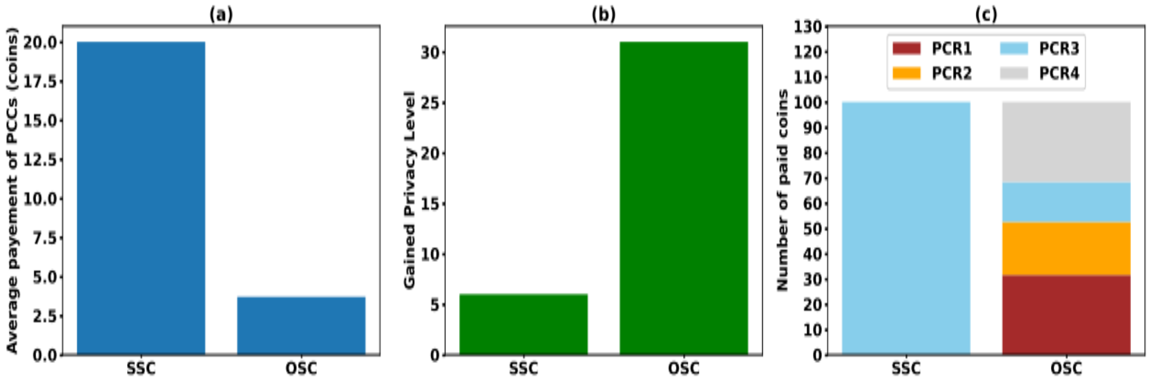


Figure 32: Comparison between the average payment (a) and privacy level (b) received by PCCs, and the cost paid by a PCR (c) participating in both PCPs under SSCs and PCPs under OSCs; (ρ= 100veh/km and sizeCZ= 60m)

C. Blockchain analysis

In this section, we first evaluate the consensus time in the consortium blockchain and carry out an analytic evaluation for selecting the first leader in the set of the consensus members. Then, we study the implementation of the proposed scheme in a real case. To calculate the average time to reach the consensus, we run an implementation of the DBFT consensus protocol developed using Python programming language in a machine equipped with a CPU (Intel i5 2.6 GHz) and 8 GO of RAM.

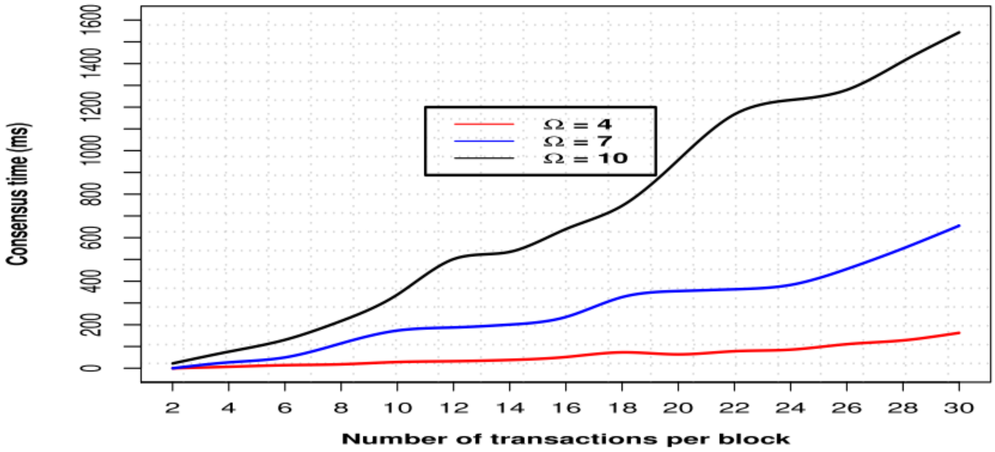


Figure 33: The average consensus time in the consortium blockchain (milliseconds)

Figure 33 illustrates the consensus time related to one PCP. In this Figure, for each curve, we fixed the number of consortium members and variated the number of transactions up 30. These transactions are generated after the execution of a SC to transfer coins/or to apply penalties. The reason why we limited the number of transactions to 30, is that the number of transactions depends on the number of cooperative vehicles inside the PCPs. Indeed, as Figures 27 and 28 show the max number of cooperative vehicles in a PCP can achieve 13 when size cz = 90m. Also, since an OSC can involve multiple PCPs and PCRs, this number of transactions can reach 30. Figure 33 shows a linear increase in the consensus time with the number of transactions. They also show that the consensus time increases with the number of consensus members. However, the consensus is reached in a short time. Indeed, it takes only 1.6 seconds to reach a consensus for a block with 30 transactions and 10 consensus members.

In the following, we consider a consortium blockchain consists of four consortium members under different traffic densities and CZ sizes. We have run a numeral evaluation to calculate their utility values for determining the first leader that initiates the consensus process. In this evaluation, the fixed parameters are set as follows: max tp = 1 s, max tc = 0.14 s, nb prop = 1, and C = 100 coins. Figure 34 shows the utility values of the consensus members calculated using the formula 23. The obtained results show that BS3 has the highest utility value among the consensus members. Thus, it will be select as the first leader.

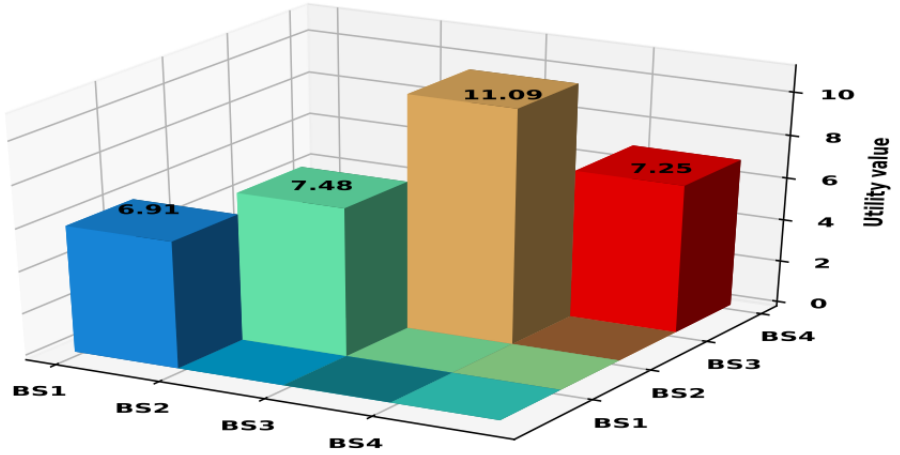


Figure 34: The utility value of four consensus members under different traffic densities and candidature zone sizes

We also consider Luxembourg as a case of the application of our scheme. In 2020, Luxembourg has started the deployment of 5G. The first stage of deployment will mainly cover Luxembourg City (5G strategy for Luxembourg, by the Ministry of State). The official geoportal of Luxembourg shows the distribution of BSs in Luxembourg city[14]. Among around 750 BSs deployed in the whole country, around 100 BSs are deployed in Luxembourg City. The city also counts around 288 thousand vehicles between local vehicles, buses, and transit vehicles circulating in the city over 24 hours (Codec et al. 2017). During the peak hour (8 am) more than 4.7 thousand vehicles can be found on the road, while at midnight (lullhour), around 700 vehicles left on roads. In the following, we estimate the number of requests that arrive from PCRs, the number of PCPs executed, and the consensus time by BS. We consider that vehicles are uniformly distributed over BSs. Therefore, at the peak hour, we count around 470 vehicles per BS, while at the lull hour, only 70 vehicles can be found under a BS. We also consider that the privacy levels of vehicles are distributed according to a normal distribution with a mean equal to the common desired privacy level of drivers. Given that vehicles tend to request for a PCP if their privacy levels go below the average, half of the vehicles under a BS can request for PCP (235 PCRs at the peak hour, 70 PCRs at the lull hour). However, as shown in Figure 35, the number of PCRs' requests that can arrive at the BS depends on the probability that PCRs request support from the scheme. In addition, the number of PCPs to be executed is limited to the number of vehicles monitored by the BS. Indeed, as shown in Figure 27, if we consider size CZ = 60 m and the traffic density = 100 veh/km, the number of collaborative of the vehicle inside the PCPs equals to 7. Thus, at the peak hour, only 68 PCPs need be executed to ensure privacy protection, while in the lull hour 10 PCPs need to be executed. As shown in Figure 35, if the request probability of PCRs is around 0.3, all PCPs are executed with the support of the scheme.

[14] https://map.geoportail.lu/theme/cadastrehertzien, accessed November11, 2020.

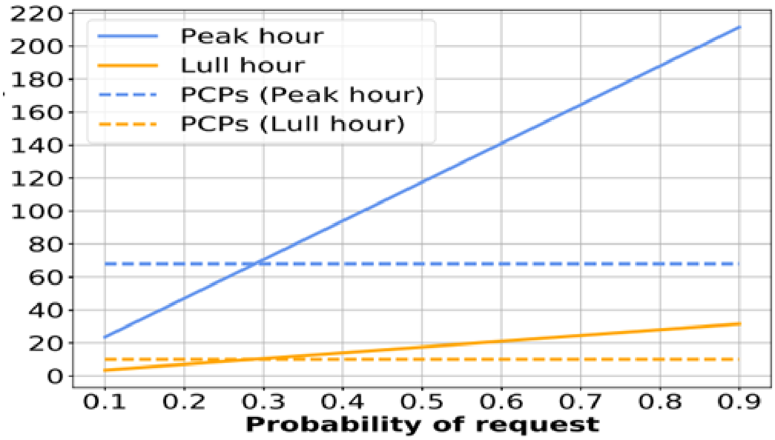
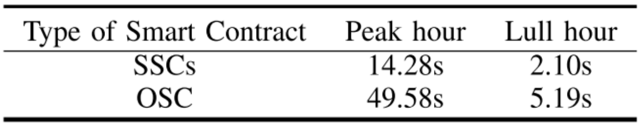


Figure 35: Potential number of PCRs' requests versus the probability of request

We also estimate consensus time under SSC and OSC. We consider that 10% of 100 the BSs deployed in the city are part of the consortium blockchain, which explains the number of consortium members considered in Figure 33. Table 19, compares cumulative consensus time under SSCs with the consensus time under an OSC for peak hour and the lull hour. The results show that in the peak hour, OSC takes a longer consensus time compared to SSCs. However, in lull hour the results show the consensus time under an OSC is close to SSCs. The consensus time can be enhanced further in the real deployment of the scheme with the high performance of 5G BS [15], and the ultra-low latency offered by 5G networks.



Type of Smart Contract	Peak hour	Lull hour
SSCs	14.28s	2.10s
OSC	49.58s	5.19s

Table 19: Comparison of consensus time for peak and lullhour under SSCs and an OSC

D. Security Game Model

In this section, we propose a security game model to capture different attacker behaviours. We consider two kinds of players, the security agent that is activated at each vehicle and BS to monitor its neighbours vehicles and BS, and malicious vehicles and infected BSs that execute the attacks defined in subsection 3.4.4.1 (C) including internal and DoS. We note that, Ψj and Ψi are the security agent and attacker players, respectively, where $i \in \{1,...,N\}$, and N is the number of attackers that attack the player Ψj, and $j \in \{1,..., M\}$, and M is the number of security agents that monitor the player Ψi. The players Ψi and Ψj have a set of strategies defined respectively as $\zeta(\Psi i)=\{\Psi i'i \mid i'=1, . . . , n'\}$ and $\zeta(\Psi j)=\{\Psi j'j \mid j'= 1, . . . , m'\}$, where n' and m' are the maximum number of strategies. The strategies of player Ψi are the number of attacks executed by the attackers against the legitimate vehicles and BSs. The strategies of player Ψj are the number of monitored vehicles and BSs that are suspected to execute the malicious behaviours cited above. Let, xi' be the probability of player Ψi to execute the strategy $\Psi i'i$ and yj' be the probability of player Ψj to launch the strategy $\Psi j'j$; where $\sum n'i'=1xi'= 1$ and $\sum m'j'=1yj'= 1$. The utility functions of the players Ψi and Ψj are shown in formulas 30 and 31.

[15] https://www.intel.com/content/www/us/en/products/processors/atom/p-series/atom-p-5900-processor-brief.html, accessed November 12,2020

$$u^t_{\Psi_j}(t) = y_{j'} * \left(\frac{ED^t - (FP^t + FN^t)}{T^t}\right) - Cost_{\Psi_j}$$

Formula 30

$$u^t_{\Psi_i}(t) = x_{i'} * \left(\frac{(FP^t + FN^t) - ED^t}{T^t}\right) - Cost_{\Psi_i}$$

Formula 31

Here, ED^t is the expected detection rate against the attackers that suspected to occur, and FP^t and F N^t are respectively the false positive and false negative rates against the suspected attacks, e.g., Ψ_j suspects the legitimate non-cooperative vehicle (and BS) as an attacker and vice versa. T^t is the total number of malicious vehicles (and BSs) that occur and target the player Ψj. Cost Ψj is the required cost of player Ψj to achieve a high level of security, high ED^t, while generating low FN^t and FP^t. CostΨi is the required cost of player Ψi to execute attacks strategies ζΨi against the player Ψj. Here, CostΨj and CostΨi ∈]0,1]. In the proposed non-cooperative game, the players Ψj run their optimal strategies $\Psi*_{j'j}$ for detecting the malicious players Ψi by taken into account the best responses of these non-cooperative players Ψi, while the malicious vehicles (and BSs) Ψi run their optimal strategies Ψ*i'i for executing the attacks by taking into account the best responses of the cooperative players Ψj. It is noted, the best response of player Ψjis the accuracy of detecting the attacks,i.e., the ED^t is high and the best response of player Ψiis executing the attacks against Ψj, without being detected,i.e., the

FP^t and FN^t are high. Therefore, the strategies couple ($\Psi*_{j'j}$,$\Psi*_{i'i}$) executed by the players Ψj and Ψi are determined by computing the optimal coordinates ($\delta*_1$,$\delta*_2$) defined as a Nash Equilibrium (NE) point (L. Zhang & Hemberg, 2019), which equals to:

$$\delta^{*1} = \underset{y_{j'}}{\operatorname{argmax}}\, u^t_{\Psi_j}(t)$$
$$\delta^{*2} = \underset{x_{i'}}{\operatorname{argmax}}\, u^t_{\Psi_i}(t)$$

Formula 32

From formula 32, we conclude that when $u^t_{\Psi i(t)}$ is equal to $\text{argmax}_{xi'}u^t_{\Psi i(t)}$, the attacker Ψ_i executes an attack such malicious PCR, PCC or BS against the player Ψj. In this case, the security agent Ψj categorizes the player Ψi as a malicious vehicle (or malicious BS), i.e., $u^t_{\Psi j(t)}$ is equal to $\text{argmax}_{yj'}u^t_{\Psi j(t)}$. As shown in Figure 36, we vary the number of iterations from 10 to 40 iterations, where at each iteration, each player aims to maximize its utility function and minimize the utility function of its opponent, i.e., the security agent aims to decrease ED^t, while FP^t and FN^t are taken into account and attacker focus to increase the FP^t and FN^t and decrease ED^t. By increasing the number of iterations, we found that there is a point of intersection of two curves (related to the functions $u^t_{\Psi i(t)}$ and $u^t_{\Psi j(t)}$, which is defined a Nash equilibrium point, ($u^t_{\Psi j(t)}$,$u^t_{\Psi i(t)}$). Therefore, when this equilibrium point is reached the security agent categorizes the malicious vehicles (or BS) with a high accuracy, i.e., detection rate and false positive rates are equals respectively to 100% and 0%.

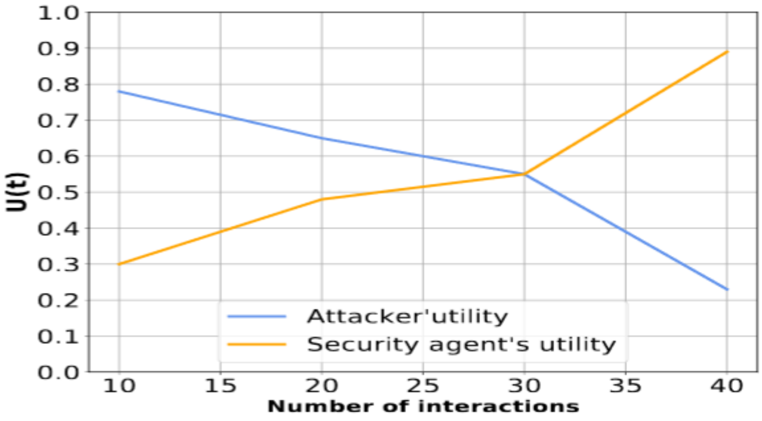


Figure 36: Nash equilibrium solution

3.4.4.6 Discussion

In this section, we discuss the incentive techniques proposed by our scheme. We then perform security, privacy, and fairness analyses. Finally, we compare between SSCs and OSCs and give some recommendations.

A. Incentive techniques

In our scheme, several incentive techniques have been proposed to stimulate non-cooperative vehicles. As shown in Figure 22 (step 9), the SC pushes vehicles to keep their reputation values positive to be able to request fora PCP. In addition, since the payments received by PCCs depend on their reputation values and their privacy levels, vehicles always try to increase their reputation values and cooperate even when their privacy levels are high to get higher payments. OSCs are another reason for vehicles to increase their reputation values through cooperation. Indeed, since the price paid by PCCs under OSCs depends on their reputation, vehicles should maintain their reputation values high to pay less when OSCs are performed. Moreover, since the consensus members are selected based on their utility, BSs will work to execute efficient PCPs to participate in the consensus processes and get coins. Also, the results show that our scheme allows more cooperative vehicles at PCPs than MPSVLP. Indeed, while our scheme can motivate more than six vehicles when sizeCZ equals 60m, MPSVLP can only motivate between three and four vehicles in a CZ of more than 100 m. Our scheme fulfils incentive and budget proprieties: (i) Individual Rationality (IR): since both PCR and PCCs will receive positives utilities in terms of privacy protection level and monetary gain respectively, (ii) Incentive compatibility (IC): since the payment of PCCs is calculated with the same formula (formula 19) whatever the smart contract is, and (iii) Budget balance (BB): since the request for a PCP is controlled by the vehicle according to its budget. In other words, vehicles can manage their requests for PCPs to ensure that their generated profits are always positive.

B. Security, Privacy & Fairness Analyses

Our scheme provides a set of security checks to thwart attackers defined in Section 3.4.4.1. For thwarting malicious PCRs, the SC verifies the PCR's balance every time it receives its request for a PCP. If a PCR sends a request without having enough coins in its balance, the SC refuses the request and decreases the PCR's reputation value. The smart contract also moves a deposit from the PCR's balance to the contract_address for ensuring the payments of PCPs. Moreover, a penalty is applied if the PCR violates any contract clause. For thwarting malicious PCCs, the SC requires PCCs to move deposits from their balances to the contract address. Penalties and reputation decreases are applied to PCCs in the case of non-respect of SC clauses. Our scheme is also thwarting malicious BSs, which try to tamper data to increase their utility for being consensus members. Indeed, our scheme stores all relevant data such as reputation values, scores, and utility values in the blockchain, which cannot be modified without a consensus process. Moreover, our scheme is based on a resilience consensus protocol where the consensus can be reached even that almost a third of BSs are faulty/malicious nodes. Attackers with fake identifiers cannot join the consortium since members should be authenticated with the CA. Furthermore, our scheme ensures accurate detection of internal and DoS attacks thanks to a game theory-based defense mechanism proposed in subsection 3.4.4.5. On the other hand, location privacy preservation of vehicles in the consortium blockchain is ensured since pseudonyms are used as sources of transactions and as account addresses as well. PCRs cannot link between two consecutive pseudonyms of PCCs. However, BSs can only link between two pseudonyms of the same vehicle for matching the feedback messages received by the invoke function with the SC. But since not all PCPs are executed with the support of our scheme, BSs cannot continually link all the pseudonyms of the vehicles. In addition, in our scheme, the accountability is maintained since only the CA can link between real identifiers of vehicles and their corresponding pseudonyms. Our scheme also ensures fairness at different levels: (i) As shown in formula 19, the payment of PCC is performed according to its current privacy level and reputation value, which ensures a fair payment system that rewards PCCs for their sacrifice and their cooperative behavior, (ii) as shown in formula 21, the contribution of each PCR in the total price of the PCP is computed according to its reputation, which is also fair since it makes sure that PCCs with higher reputation values contribute less in the total price, and (iii) As shown in formula 19, the calculation of utility of BS takes into the account the reputation values of vehicles, which ensures fair weights of vehicles' feedback used in the calculation of utility values. On the other hand, there is no fairness issue if certain vehicles travel more than the others. Since as long as vehicles are travelling, they will have more opportunities to participate PCPs, but also their privacy levels will decrease.

C. SSC vs OSC

Our scheme proposes two types of smarts contracts: SSCs and OSCs. Our evaluation results show that OSCs allows reducing the number of SCs managed by the scheme and decreasing the costs paid by PCRs compared to SSCs. They also show that while the payment received by a PCC under an OSC is lower than the payment received under an SSC, the location privacy level is better under an OSC. However, the creation of OSCs takes more longer than SSCs since BSs need to wait a certain time to collect requests for PCRs, which may result in an excessive delay for executing PCPs on time. Therefore, our recommendations are to adapt the duration of PCRs' requests collection (ΔT1) according to the number of requests and the maximum time allowed to execute the PCP. The results also show that OCSs have a longer consensus time than SSCs, especially peak traffic hours.

3.4.5 SDN-based privacy protection framework for 5G Vehicular Networks

While the adoption of connected vehicles is growing, security and privacy concerns are still the key barriers raised by society. These concerns mandate automakers and standardization groups to propose convenient solutions for privacy preservation. One of the main proposed solutions is the use of Pseudonym-Changing Strategies (PCSs). However, ETSI has recently published a technical report which highlights the absence of standardized and efficient PCSs (ETSI TR 103 415). This alarming situation mandates an innovative shift in the way that the privacy of end-users is protected during their journey. Software Defined Networking (SDN) is emerging as a key 5G enabler to manage the network in a dynamic manner. SDN-enabled wireless networks are opening up new programmable and highly-flexible privacy-aware solutions. We exploit this paradigm to propose an innovative software-defined location privacy architecture for vehicular networks. The proposed architecture is context-aware, programmable, extensible, and able to encompass all existing and future pseudonym-changing strategies. To demonstrate the merit of our architecture, we consider a case study that involves four pseudonym-changing strategies, which we deploy over our architecture and compare with their static implementations. We also detail how the SDN controller dynamically switches between the strategies according to the context.

3.4.5.1 Pseudonym-Changing Strategies: Standardization Efforts and Open Issues

Security standardization bodies have agreed to adopt PCS to protect the location privacy of connected vehicles. However, while in the US, the Society of Automotive Engineers (SAE) suggests that vehicles change their pseudonym every five minutes (SAE International, 2016), the European telecommunications standardization organization, ETSI, does not suggest the adoption of any PCS (SAE International, 2016). In the light of this, many PCSs are proposed in the literature. In (Abdelwahab Boualouache et al., 2017), we presented a comprehensive survey and classification of these strategies. This paper also highlights open issues and presents recommendations, including the importance of developing a dynamic system to select the applying PCS according to the vehicular context. Recently, ETSI published a technical report (ETSI TR 103 415) that presents a pre-standardization study of PCS (SAE International, 2016). This document surveys the existing categories of strategies. It also discusses and describes the suggestions of the European projects (PRESERVE, SCOOP@F, and C2C-CC) regarding PCS. The document identifies the open issues of PCSs and proposes a set of recommendations addressing these issues. In the following, we discuss the open issues highlighted in SAE Standards(SAE International, 2016) and by (Abdelwahab Boualouache et al., 2017) and the related recent advances:

- **Impact on road safety**: as shown in (Abdelwahab Boualouache et al., 2017), strategies using radio silence are the most efficient solutions. However, their major drawback is their significant negative impact on safety-related applications. This was first investigated in Vehicular Networking Conference in 2013 (Lefevre et al., 2013), where the authors recommend that the silent period should be shorter than two seconds and that long silent periods can result in hazardous situations since many safety messages will not be transmitted due to radio silence. The ETSI technical report (SAE International, 2016) also discusses the problems of “missing vehicles" and “guest vehicles". Missing vehicles are those that put radio silence into effect after changing their pseudonyms; at the end of this period, these vehicles suddenly appear in the LDMs (Local Dynamic Map) of neighboring vehicles. This may generate unpredictable reactions as highlighted in SAE Standards J2945/1. In contrast, the problem of the guest vehicle is observed when a vehicle changes its pseudonym while its old pseudonym still populates the LDMs of its neighboring vehicles (Jemaa et al., 2017). Subsequently, LDM messages contain two entries that correspond to the same vehicle, leading to a misinterpretation of the surrounding environment by neighbouring vehicles. Unlike the missing vehicle problem, the ghost vehicle problem is not only linked to radio silence based strategies but to PCSs in general.
- **Non-cooperative behaviour**: by triggering the change of their pseudonyms at the same time slot, cooperative vehicles ensure a high level of anonymity and create confusion for the attacker. Consequently, the existence of non-cooperative vehicles will significantly hinder the efficiency of the PCS, specifically under lower vehicular density. The authors of “Non-cooperative location privacy” (Freudiger et al., 2009) study PCSs under a non-cooperative environment. They propose a game theory model and find a Nash equilibrium of the PCS under different types of games (static/dynamic, with and without complete information). Other works such as by (Garey & Johnson, 1990) and by (Ying et al., 2015) propose incentive mechanisms to motivate non-cooperative vehicles to participate in the PCS.
- **Attacker model**: It is not trivial to estimate the power of tracking attackers that may exist in the future deployment of vehicular networks. Attacker power can be expressed in terms of tracking capabilities (strong or weak sniffing stations, the efficiency of the tracking algorithm, etc.) and the coverage area. In addition, it is critical to properly define a realistic attacker model. For this reason, most of the proposed PCSs have assumed the extreme case of the attacker model (global attacker full of capabilities); however, this assumption is not realistic because global coverage entails a significant surveillance cost. Consequently, the authors J. Petit et al. at “Connected vehicles: Surveillance threat a mitigation.”(Petit et al., 2015) propose a mid-sized attacker whose power is in between that a local attacker and a global one. They also distinguish three tracking periods (i.e short-term, mid-term, and long-term) and two levels of surveillance granularity (i.e Road-level and Zone-level).
- **Evaluation metrics**: many metrics are proposed to assess the performance of PCSs. The recent study carried out by (Zhao & Wagner, 2019) shows that there is no single privacy metric that outperforms all others under different contexts (mobility, traffic conditions, road

section, etc.). For this reason, it is recommended to combine all metrics to obtain a fair performance evaluation of a PCS.

- **Privacy model**: the privacy level depends mainly on the considered attacker model and the evaluation metrics. The authors of “Connected vehicles: Surveillance threat and mitigation” proposed a linear model to quantify the loss of privacy after the last change of pseudonym. In this model, the privacy level of vehicles linearly decreases according to a sensitivity parameter, which characterizes the power of the adversary. However, this model has two major drawbacks: (i) it does not specify how the sensitivity parameter is measured. (ii)the linearity of this model is not justified.
- **Sybil attacks**: In this attack, vehicles use multiple identities, called Sybils, which can be exploited to create a fake traffic jam and hence to alter other vehicles’ perceptions. Pseudonyms could be exploited to launch Sybil attacks. The ETSI technical report (SAE Standards 2016, J2945/1) gives some recommendations on thwarting Sybil attacks, such as setting the maximum number of pseudonyms that can be used simultaneously and the minimum duration for which the pseudonyms should be used. The technical report also recommends the use of misbehavior detection systems.
- **Pseudonym lock**: ETSI standards specify that the PCS could be locked on-demand for a maximum of 255s, in particular when a critical safety situation occurs. The priority levels of such a situation are respectively “0" or “1" (ETSI, 2013b). PCS locking is also proposed by the SAE. However, the conditions when the pseudonyms are locked are not yet defined.
- **Pseudonym reuse**: Although the reuse of pseudonyms minimizes the storage capacity and facilitates the management of pseudonyms, it can decrease the level of privacy. Therefore the reuse of pseudonyms is not recommended as a privacy best practice. However, the Car2car consortium considers the reuse of pseudonym while defining some KPI to increase the privacy level (Abdelwahab Boualouache et al., 2017).

3.4.5.2 Proposed Architecture: Building blocks

Our self-privacy-preserving architecture leverages the SDN paradigm and thus follows its main principle, which is the separation between the data and the control plane. The control plane is responsible for dynamically selecting the PCS, adjusting the parameters of strategy, and planning the strategy rules. On the other hand, the data plane translates the defined rules into actions to apply the PCS. The communications between the control plane and the data plane are secure.

A. Control Plane

Figure 37 shows the logical modules of the control plane in our architecture. The PCS module receives a demand from the application layer to provide the location privacy service. This module chooses the most convenient PCS to be executed based on the information received from two modules: The Mobility and Topology module and the Attacker Model module. Once the strategy is selected, the PCS module invokes (i) the Parameter Settings module to request the parameters of the strategy; (ii) the Incentive Model module to request the appropriate incentive method to motivate non-cooperative vehicles; and (iii) the Privacy Metric module to request indicators and KPIs for the evaluation of PCS performance. In the following, we detail these modules.

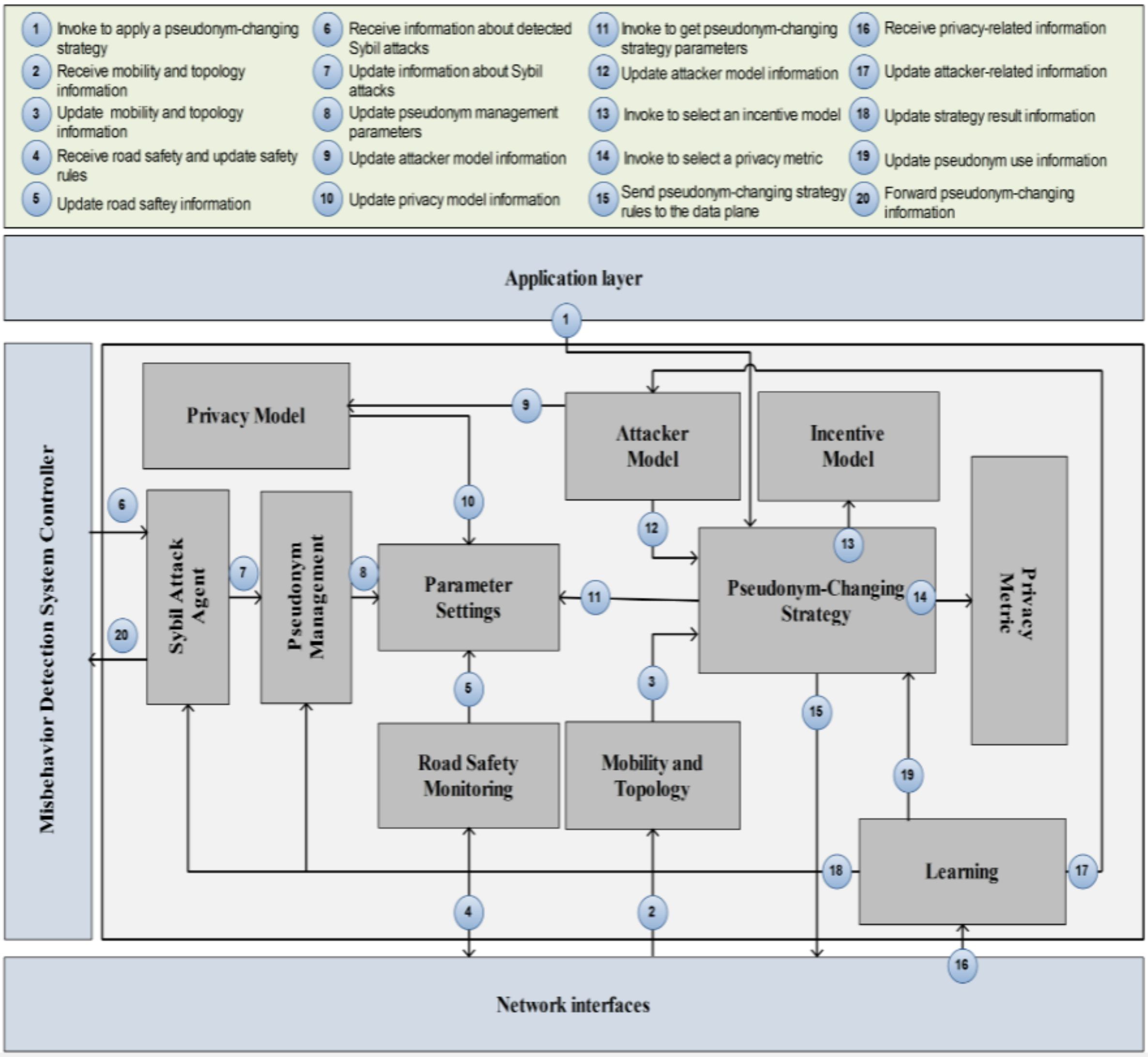

1 Invoke to apply a pseudonym-changing strategy
2 Receive mobility and topology information
3 Update mobility and topology information
4 Receive road safety and update safety rules
5 Update road saftey information
6 Receive information about detected Sybil attacks
7 Update information about Sybil attacks
8 Update pseudonym management parameters
9 Update attacker model information
10 Update privacy model information
11 Invoke to get pseudonym-changing strategy parameters
12 Update attacker model information
13 Invoke to select an incentive model
14 Invoke to select a privacy metric
15 Send pseudonym-changing strategy rules to the data plane
16 Receive privacy-related information
17 Update attacker-related information
18 Update strategy result information
19 Update pseudonym use information
20 Forward pseudonym-changing information
Application layer
Misbehavior Detection System Controller
Privacy Model
Attacker Model
Incentive Model
Sybil Attack Agent
Pseudonym Management
Parameter Settings
Pseudonym-Changing Strategy
Privacy Metric
Road Safety Monitoring
Mobility and Topology
Learning
Network interfaces

Figure 37: The logical modules of the control plane and the interactions between them

- **Road Safety Monitoring**: this module monitors road conditions and their impact on traffic safety. Based on this assessment, the module develops appropriate SDN rules which are sent to the data plane. In addition, this module provides the necessary information to the Parameter Settings module to tune the PCS parameters, such as the duration of radio silence and the lock period.
- **Misbehavior Detection System Controller**: this is an external component, which detects misbehaving attacks such as message injection, denial of service (DoS) and Sybil attacks. The SDN controller of our self-privacy-preserving architecture uses the information received from the Misbehavior Detection System Controller to update its parameters in order to limit Sybil attacks and returns information to help in detecting Sybil attacks and accurately evaluating the trust levels of vehicles.
- **Sybil Attack Agent**: this interface is used to interact with the Misbehavior Detection System Controller, receiving information from it and forwarding it to the Pseudonym Management module to adjust some PCS parameters. It also receives information from the Learning module and forwards this to the Misbehavior Detection System Controller to enhance the attack detection ratio.
- **Pseudonym Management**: this module plans the rules that orchestrate the use of pseudonyms: the reuse of pseudonyms, the frequency of changing of pseudonyms, the number of pseudonyms that can be used in parallel, etc. This module receives information

from both the Sybil Attack Agent and learning modules and sends the resulting rules to the Parameter Settings module.

- **Privacy Model**: This is used to model the loss of privacy of vehicles over time. As explained in the previous section, the loss of privacy mainly depends on the strength of the attacker model. For this reason, this module receives input from the Attacker Model module. The Privacy Model provides input to the Parameter Settings module, which in return specifies the parameters of the Privacy Model.
- **Mobility and Topology:** this module monitors the mobility pattern of vehicles and the road topology in real time.
- **Parameter Settings**: this module sets the different parameters of the PCS, such as the duration of the radio silence period and the minimum duration of the use of pseudonyms. The definition of these parameters is made according to the information received from the Road Safety, Pseudonym Management, and the Privacy Model modules.
- **Attacker Model**: this module evaluates the power of the attacker. As discussed in the previous section, the attacker can be internal or external, local, or mid-sized, long-term. It can perform simple syntactic linking of pseudonyms but can also carry out more advanced semantic linking of pseudonyms. This module gets regular updates from the learning model and sends feedback to the Pseudonym-Changing Strategy module.
- **Incentive Mode**l: this module defines the incentive model, which is used to motivate selfish vehicles to participate in the PCS.
- **Privacy Metric**: this module defines the privacy metrics used to evaluate the PCS. It worth mentioning that the privacy metrics can be selected by the PCS to evaluate its own performance
- **PCS Module**: this module defines the strategy to be executed based on the information received from the Mobility and Topology module and the Attacker Model module. Once the strategy is selected, this module invokes the ParameterSettings module to obtain the most appropriate parameters of the selected strategy. This module also invokes the Privacy Metric module and the Incentive Model module to select the evaluation metric and the incentive method, respectively.
- **Learning:** this module periodically receives privacy-related information from the data plane (i.e. the privacy levels of vehicles, the presence of an attacker, and the set of selfish vehicles). This information is analyzed and forwarded to the corresponding modules: (i) the Attacker Model module to adjust the attacker model being used; (ii) the PCS module to tune the strategy parameters, and the Incentive Model module, and to select an additional potential privacy metric. (ii) the Pseudonym Management module to adjust pseudonym management related parameters, and finally (iv) the Sybil Attack Agent, which forwards pseudonym-changing information to the Misbehavior Detection System Controller. The purpose is to support this controller in the accurate detection of Sybil attacks and trust assessment of vehicles.

B. Data Plane

The data plane is composed of the different vehicles that are involved in the PCS. Figure 38 depicts the modules of the data plane, which are responsible for the execution of the PCS. The data plane uses the vehicles' communication interfaces to collect pertinent information concerns the surrounding vehicular environment. The data plane sends mobility, safety, and privacy information to the control plane, while it receives safety and strategy rules. In the following, we describe the modules and the databases of the data plane:

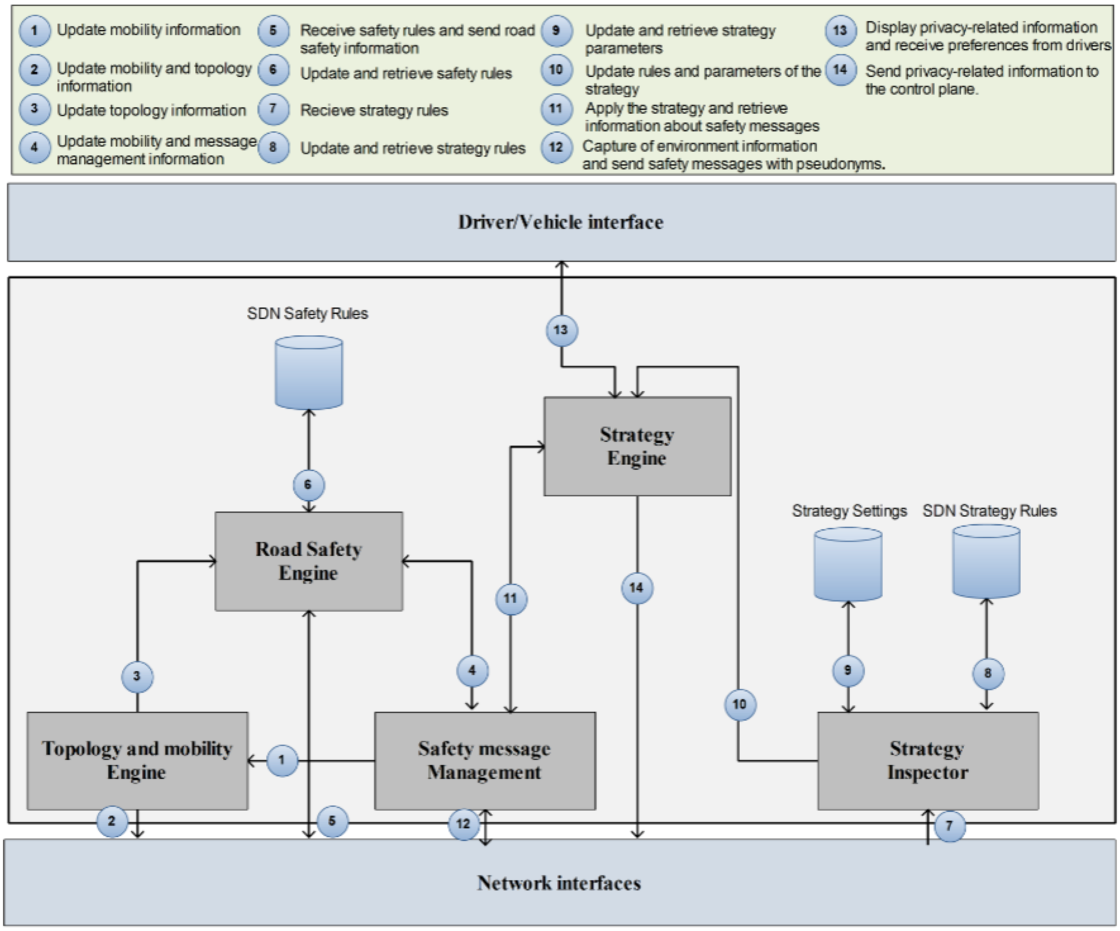

1 Update mobility information
2 Update mobility and topology information
3 Update topology information
4 Update mobility and message management information
5 Receive safety rules and send road safety information
6 Update and retrieve safety rules
7 Recieve strategy rules
8 Update and retrieve strategy rules
9 Update and retrieve strategy parameters
10 Update rules and parameters of the strategy
11 Apply the strategy and retrieve information about safety messages
12 Capture of environment information and send safety messages with pseudonyms.
13 Display privacy-related information and receive preferences from drivers
14 Send privacy-related information to the control plane.
Driver/Vehicle interface
SDN Safety Rules
Strategy Engine
Road Safety Engine
Strategy Settings
SDN Strategy Rules
Topology and mobility Engine
Safety message Management
Strategy Inspector
Network interfaces

Figure 38: The logical components of the data plane and the interactions between them

- **Safety Message Management**: this module sends and receives pseudonymous safety messages. It also receives instructions from the Strategy Engine. These instructions vary according to the applied strategy. In addition, this module provides the status of the surrounding environment and the impact of the applied PCS to the Road Safety Engine, the Topology, and the Mobility engine, and finally to the Strategy Engine.
- **Mobility and Topology Engine**: Equipped with a map and GPS, this module sends the mobility information of the vehicle such as position, speed, and acceleration and the topology information to the Road Safety Engine and to the control plane.
- **SDN Safety Rules**: This is a database, which contains the safety rules that are used to assess road conditions. The rules data is received from the control plane.
- **Road Safety Engine**: this module receives, stores, and updates the safety rules received from the control plane. These rules are used to evaluate road safety based on the information received from the Topology and Mobility Engine and the Safety Message Management module. This module periodically sends road safety information to the control plane.
- **SDN Strategy Rules**: This is a database that contains the rules related to PCS. These rules describe where, when, and how pseudonyms change. The database is regularly updated by the Strategy Inspector module; based on the information received from the control plane.
- **Strategy Settings**: This is a database that contains the settings of the applied strategy, such as the duration of the radio silence period after the changing of the pseudonym. This database is also regularly updated by the Strategy Inspector module according to the information received from the control plane.
- **Strategy Inspector**: This module represents an interface, which communicates with the PCS module of the control plane. It receives information from the SDN controller(s) and stores

them in two databases: the SDN Strategy rules and the Strategy Settings databases. This module also forwards these PCS rules and settings to the Strategy Engine module.

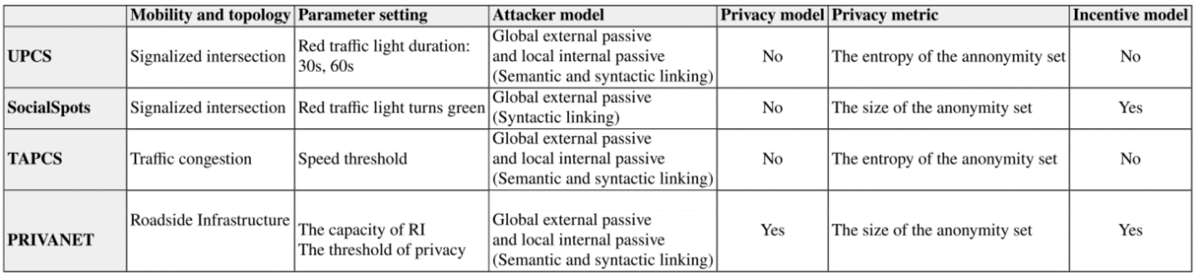
- **Strategy Engine**: this module executes the PCS according to the rules and settings received from the Strategy Inspector module. To execute the strategy, the module continuously monitors and sends instructions to the Safety Message Management module. This module provides privacy protection related information to the driver from whom it receives privacy level recommendations. This module also sends privacy-related information to the control plane.

3.4.5.3 Case Study

To demonstrate the merit of our proposed architecture, we conducted the following case study. As shown in Figure 39 (1), we populated a Software-Defined Location Privacy Controller (SDLP) with four state-of-the-art PCSs: UPCS (Abdelwahab Boualouache & Moussaoui, 2016), TAPCS (Abdelwahab Boualouache & Moussaoui, 2017), PRIVANET (A. Boualouache et al., 2020) and SocialSpots (Lu et al., 2012). In this section, we first show how these strategies are integrated into our architecture. Then, we illustrate how the SDLP performs a context-aware PCS selection. The context is mainly defined by mobility and topology, as well as the attacker model. Finally, we conduct a simulation-based study to demonstrate how our proposed architecture dynamically updates the security parameters of each strategy.

A. PCSs Deployment

Our proposed architecture is flexible enough to support any state-of-the-art PCS. Table 20 shows how the considered strategies are mapped to our architecture. This table has six columns: (i) Mobility and topology: specifies the topology where the strategy can be used; (ii) Parameter Setting: specifies the parameters of the strategy; (iii) Attacker model: specifies that attacker model from which the strategy provides protection; (iv) Privacy model: specifies if the strategy uses a privacy model or not;(v) Privacy metric: specifies the metric used to evaluate the strategy; (vi) Incentive model: specifies if the strategy uses an incentive model or not.



	Mobility and topology	Parameter setting	Attacker model	Privacy model	Privacy metric	Incentive model
UPCS	Signalized intersection	Red traffic light duration: 30s, 60s	Global external passive and local internal passive (Semantic and syntactic linking)	No	The entropy of the annonymity set	No
SocialSpots	Signalized intersection	Red traffic light turns green	Global external passive (Syntactic linking)	No	The size of the anonymity set	Yes
TAPCS	Traffic congestion	Speed threshold	Global external passive and local internal passive (Semantic and syntactic linking)	No	The entropy of the anonymity set	No
PRIVANET	Roadside Infrastructure	The capacity of RI The threshold of privacy	Global external passive and local internal passive (Semantic and syntactic linking)	Yes	The size of the anonymity set	Yes

Table 20: The deployments of PCSs in the self-privacy-preserving architecture

Control plane modules are activated or deactivated according to the requirements of each PCS. For example, the Incentive Model module is disabled for UPCS and TAPCS since these strategies do not propose any mechanism to motivate non-cooperative vehicles to change their pseudonyms; while the Privacy Model module is only activated for PRIVANET strategy.

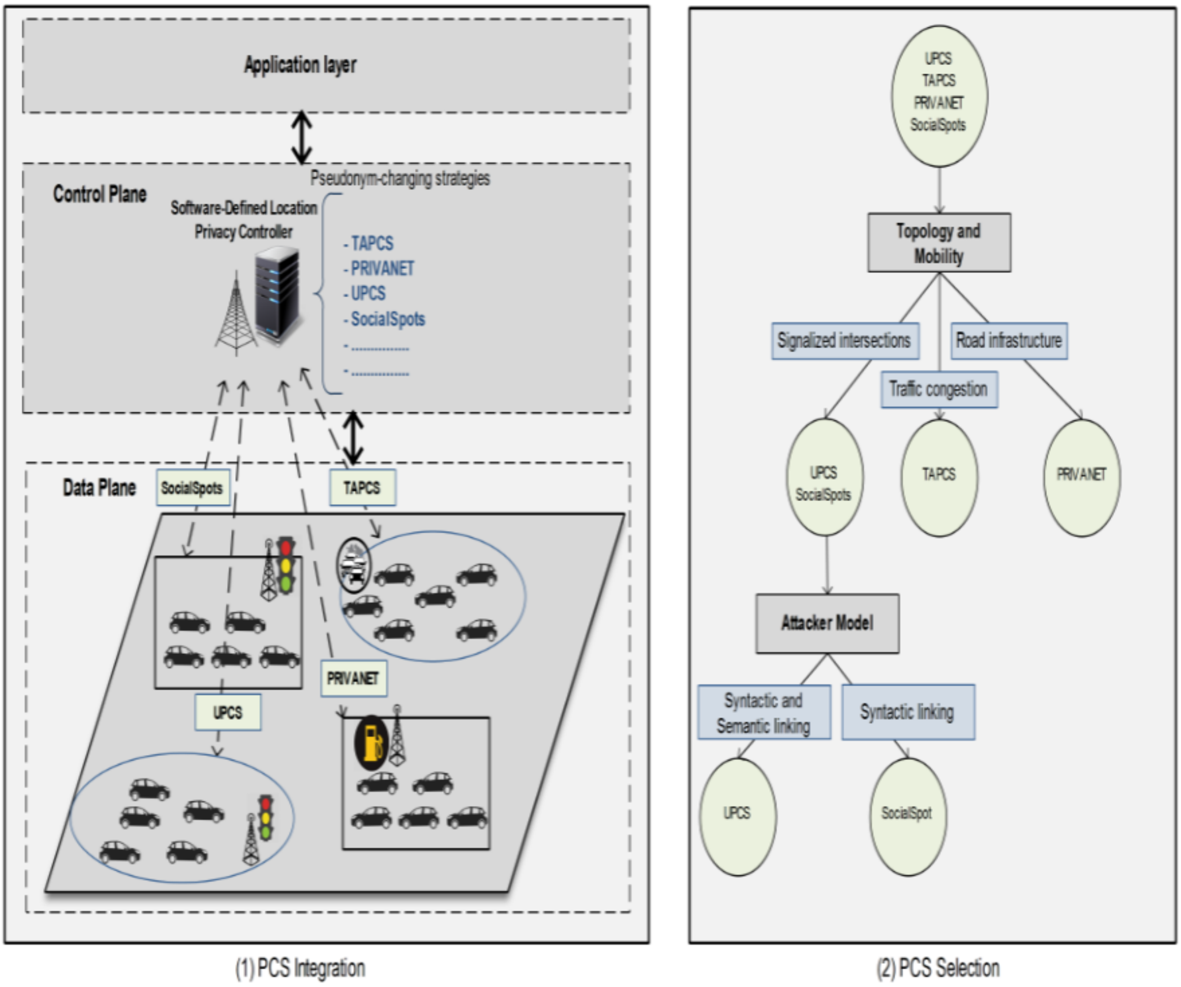
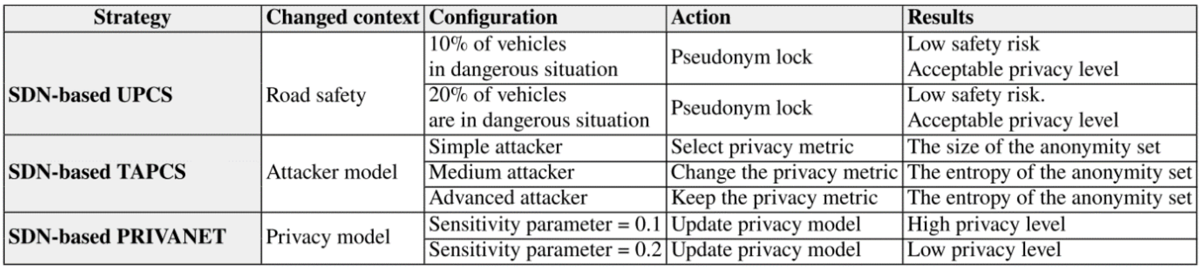


Figure 39: The selection of pseudonym changing strategy

Figure 39 (2) illustrates the different steps of the selection of a PCS. The SDLP first checks the information received from the Mobility and Topology module. For instance, if the vehicle is entering a signalized intersection, two PCSs could be applied to this context: UPCS and SocialSpots. To decide which of the two strategies to apply, SDLP checks information received from the Attacker Model module. If the attacker model can perform both syntactic and semantic pseudonym linking attacks, then UPCS is selected. Otherwise, if the attacker can perform only syntactic attacks, SocialSpots is selected. More details on syntactic and semantic pseudonym linking attacks can be found in (Abdelwahab Boualouache et al., 2017).

B. Simulation Setup

We carried out a simulation-based analysis to demonstrate the merit of our SDN-based and self-learning architecture and how it dynamically adapts the PCS security parameters to the context. This simulation-based analysis was performed using Veins Simulation Framework (Sommer et al., 2011). The considered scenario is similar to that proposed in “Computers and Intractability; A Guide to the Theory of NP-Completeness” by (Garey & Johnson, 1990). Three strategies are simulated: UPCS, TAPCS, and PRIVANET. SocialSpots was excluded, as it has the same application context (signalized intersections) as UPCS.



Strategy	Changed context	Configuration	Action	Results
SDN-based UPCS	Road safety	10% of vehicles in dangerous situation	Pseudonym lock	Low safety risk Acceptable privacy level
		20% of vehicles are in dangerous situation	Pseudonym lock	Low safety risk. Acceptable privacy level
SDN-based TAPCS	Attacker model	Simple attacker	Select privacy metric	The size of the anonymity set
		Medium attacker	Change the privacy metric	The entropy of the anonymity set
		Advanced attacker	Keep the privacy metric	The entropy of the anonymity set
SDN-based PRIVANET	Privacy model	Sensitivity parameter = 0.1	Update privacy model	High privacy level
		Sensitivity parameter = 0.2	Update privacy model	Low privacy level

Table 21: The configuration of pseudonym-changing strategies

Table 21 details the configurations of the simulated strategies. This table has four columns: (i) Changed context: specifies the context we change during the simulation;(ii) Configuration: specifies the values we assign to the context' parameters; (iii) Action: specifies the action to perform when the parameter is changed; (iv) Results: specifies the obtained results when the action is applied. To demonstrate the dynamic changing of PCS parameters according to context, three different scenarios are considered.

1. **Scenario 1**: uses UPCS strategy in a road safety context, where the number of vehicles in a dangerous situation can be 10% or 20%. The pseudonym changing in such a situation can generate traffic collisions and accidents.
2. **Scenario 2**: uses TAPCS strategy, where we study how this strategy adapts the privacy metric to the attacker model. Three configurations of the attacker model are considered: simple, medium, and advanced.
3. **Scenario 3**: uses PRIVANET focusing on the privacy model. We consider two configurations of this model by varying the sensitivity parameter value, which characterizes the power of the adversary.

C. Simulation Results

Figure 40 compares the static implementation UPCS (static UPCS) to its SDN-based variant (SDN-based UPCS). Two performance indicators are considered: the privacy level and safety. As shown in Figure 40, static UPCS provides a higher level of privacy protection compared to SDN-based UPCS. However, SDN-based UPCS has a lower safety risk than static UPCS. The reason for this, as described in Table 21, is that SDLP takes an action to lock pseudonym-changing processes of vehicles in a dangerous situation. This lock slightly decreases the privacy protection level while reducing the safety risk. Figure 41 makes a comparison between Static TAPCS and SDN-based TAPCS.

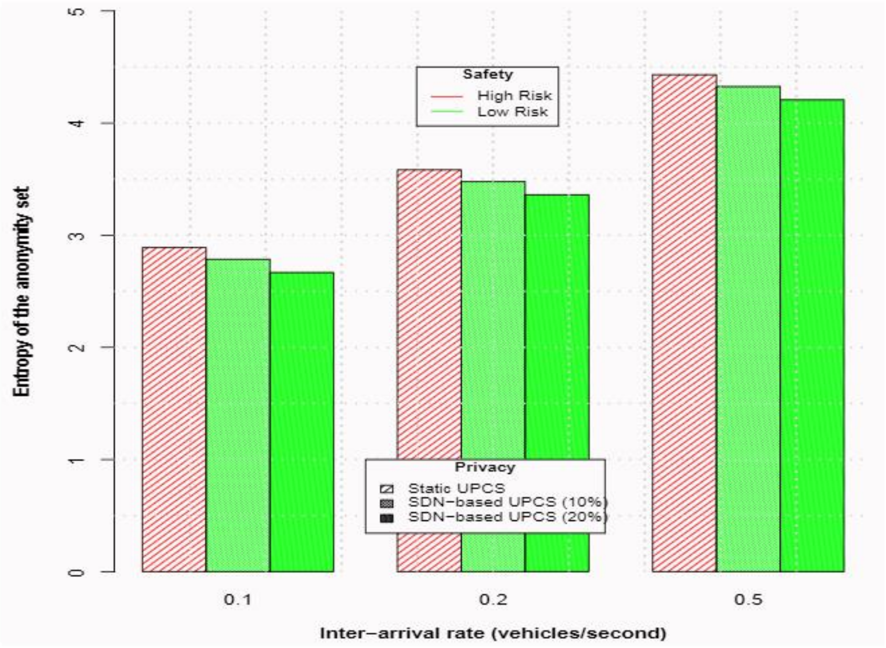


Figure 40: Static UPCS vs SDN-based UPCS

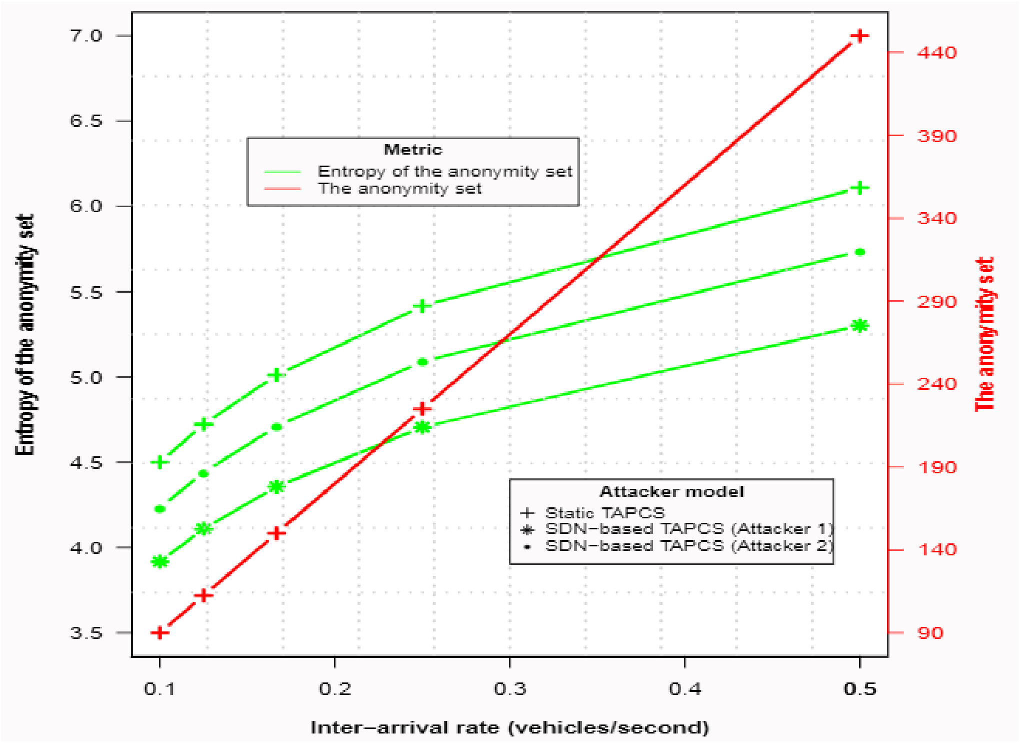


Figure 41: Static TAPCS vs SDN-based TAPCS

In Static TAPCS, the entropy of anonymity set is used as a performance metric, whatever the used attacker model. However, the SDN-based TAPCS varies the performance metric according to the power of the attacker. For instance, the size of the anonymity set is chosen when the attacker is simple, while the entropy of the anonymity set is considered when the attacker is medium or advanced. This selection of the performance metrics is based on the probabilities of distinction between vehicles in the considered area. In the former case, these probabilities are equal and hence the measuring size of the anonymity set performs well. In the latter case, these probabilities are not equal; hence the need to take the entropy into account.

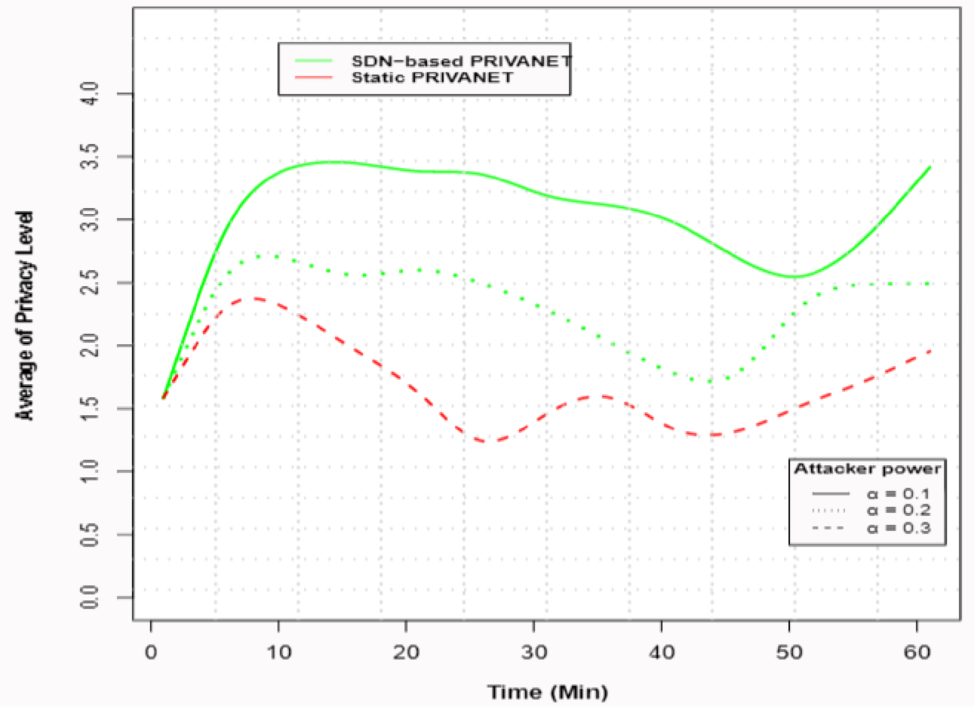


Figure 42: Static PRIVANET vs. SDN-based PRIVANET

Finally, we compare the static implementation of PRIVANET and the SDN-based version. As illustrated in Figure 42, the sensitivity parameter (α), which characterizes the power of the attacker, remains unchanged in Static PRIVANET and is equal to 0.3. However, for SDN-based PRIVANET, the sensitivity parameter is updated according to the information received from the data plane. The change in the power of the attacker (the sensitivity parameter) has a direct impact on the privacy level obtained by vehicles. Indeed, as illustrated in Figure 42, the high values of the average of privacy are obtained when the sensitivity parameter equals 0.1. However, the lower values of the average of privacy are obtained when the sensitivity parameter equals 0.3.

3.4.6 Blockchain-SDN based data trading scheme in 5G Vehicular Fog Computing

The size and variety of data collected by connected vehicles have enabled new data trading business models. However, lack of trust, scalability, privacy, and flexibility are among the main obstacles to build successful vehicular data trading services. In this solution, we leverage Software-Defined Networking (SDN) and blockchain to propose a novel scalable and secure data trading scheme for 5G enabled Vehicular Fog Computing. The scheme's blockchain system consists of SDN controllers, which relies on a resilient and lightweight consensus protocol to ensure fast and reliable block mining and validation. We design a secure and fair data trading smart contract between data requesters (vehicles) and data providers (vehicles). We also combine the SDN and a genetic algorithm for dynamic and context-aware placement of fog stations. Moreover, we analyze the scheme's fairness and monetary incentives based on the Stackelberg game model. The performance analysis is performed based on a real deployment case. It shows that our scheme provides: (1) effective and efficient data trading; (2) secure, private, and fast validation of blocks; and (3) optimal and fair monetary price management.

3.4.6.1 Blockchain-SDN Based Architecture For 5G Vehicular Data Trading

In this section, we present our blockchain-SDN based architecture for data trading in 5G vehicular fog computing. This section is structured as follows. We first describe the considered system model. We then present the system's initialization.

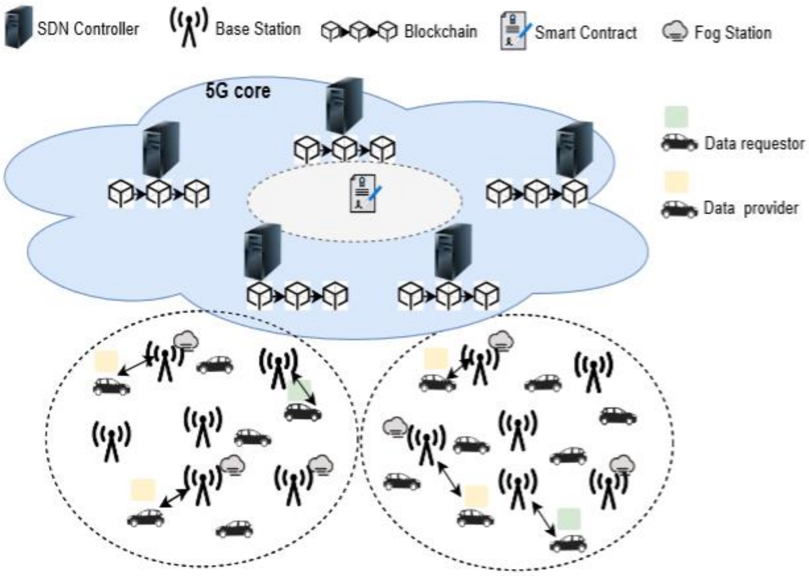


Figure 43: Blockchain-SDN based architecture for data trading in5G vehicular fog computing

A. System Model

As illustrated in Figure 43, we consider a 5G vehicular fog computing architecture consisting of three layers:

- **The infrastructure layer**: this includes vehicles equipped with sensors to collect data from the surrounding environment. Each vehicle is also equipped with a V2X interface to communicate with nearby vehicles and with 5G Base Stations (BSs). The communication in this layer is multi-hop Vehicle-to-Vehicle (V2V). Vehicle-to-Infrastructure (V2I) communications are used to communicate with the other layers.
- **5G-fog layer**: this consists of several BSs acting as fog nodes with sufficient data storage, processing, and computing capabilities, and distributed over a specific geographic perimeter. All BSs are connected through secure 5G links.
- **SDN control layer**: this layer is located above two previous layers. It includes a set of regional SDN controllers (SDNCs) hosted on the 5G core network. Each SDN controller (sdnck) controls a specific geographic area consists of a set BSs. Each sdnck has also global knowledge of such things as the mobility of vehicles and the density of the controlled area. In addition, each sdnck is equipped with a consortium blockchain hosting transactions and smart contracts for enabling reliable data sharing and secure data trading between vehicles. All SDNCs are connected through secure 5G links. Communication links between SDNCs and BSs are also secured.

In our scheme, the control plane is made up of SDNCs, which are mainly responsible for: (i) The establishment of the smart contract between data requests and data providers as described in subsection 3.4.4.3, (ii) the negotiation of the optimal data trading price and fair payment that ensure the maximum utilities for data trading participant as described in Section 3.4.4.6, and (iii) ruining consensus processes to ensure the mining and the insertion of blockchain blocks as described in subsection 3.4.6.1, (iv) A mobility-aware deployment of fog stations, which dynamically place fog stations as near as possible to vehicles as described in Section 3.4.6.3., and (v) Data routing and migration, which defines the routes that the data will follow from its origin (vehicles) to its destination (fog stations) and migrate data from a fog station to another (Ji et al 2016).

In a vehicular data trading scenario, vehicles send their data requests to data providers. However, malicious data providers can supply false or low-quality data, and on the other hand, data requesters may not pay for the service. Furthermore, due to high mobility and density characterized vehicular networks, disconnections can occur, and therefore data delivery might not be ensured. Consequently, vehicles can ask for support from our scheme. Indeed, the 5G fog and blockchain layers are acting as a controller of vehicular data trading transactions. All vehicles involved in these transactions are recorded in the blockchain and are protected by smart contracts. The fog layer allows the rapid processing of end-to-end data trading procedures. In the following, we define a data requester (DR) as each vehicle requests data. We also define a Data provider (DP) as each vehicle that provides the data.

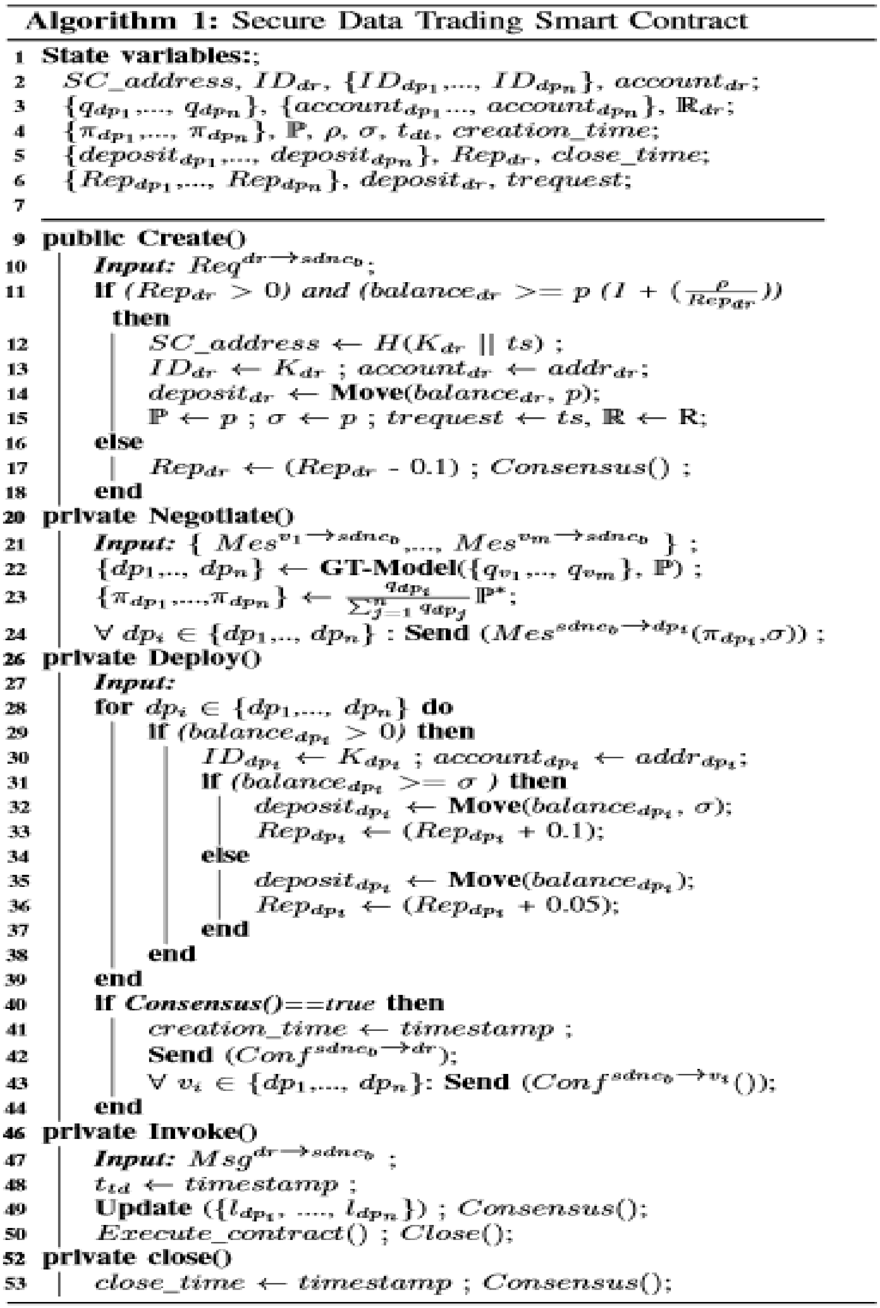
B. System Initialization

To implement a secure and privacy-preserving vehicular data trading, before joining to the system, vehicles, BSs and SDNCs register with the Certification Authority (CA). Specifically, during the registration, each vehicle vi is equipped with a private key SK_{vi}, a public key PK_{vi}, and a public certificate $Cert_{vi}$, respectively. In addition, each bsji s equipped a private key SK_{bsj}, a public key PK_{bsj}, and a public certificate $Cert_{bsj}$, respectively. Moreover, each sdnck is equipped a private key SK_{sdnck}, a public key PK_{sdnck}, and a public certificate $Cert_{sdnck}$, respectively. On the other hand, each vehicle vi also gets an account accountvi, which includes its wallet address addressvi, its account balance $balance_{vi}$, its reputation value Repvi, and the data quality level l_{vi}. To ensure the authentication and integrity of information, asymmetric encryption is used in the architecture. Each vehicle vi is pre-loaded with a set of s pseudonyms Kvi,k where k∈1, ..., s, which are public keys certified by the CA. For each pseudonym Kvi,k, the CA provides a certificate $Cert_{vi,k}(K_{vi,k})$. Messages are properly signed with a private key$K^{-1}_{vi,k}$ corresponding to the pseudonym $K_{vi,k}$. A certificate is attached to each message to enable other vehicles to verify the sender’s authenticity. To maintain the privacy of vehicles in the blockchain, pseudonyms considered as account addresses and the source addresses for verifying the authenticity of transactions.

3.4.6.2 Vehicular Data Trading Smart Contract

A. Smart Contract Design

In this section, we design a smart contract (SC) aiming at ensuring secure data trading between vehicles and motivating DPs to participate in data trading operations. Each SC has a unique contract address ($SC_{address}$) and maintains a set of state variables including the identifier of the DR (ID_{dr}), a set of data requirements (Rdr) expressed by DR, the account address of the DR (accountdr), the identifiers of DPs $\{ID_{dp1},...,ID_{dpn}\}$, the account addresses of DPs $\{account_{dp1},...,account_{dpn}\}$, and the quantities of data provided by each DP $\{q_{dp1},...,q_{dpn}\}$. The SC also includes the price of the data trading operation P (the total number of coins that DR pays for DPs), the number of coins to pay for each DP $\{\pi_{dp1},...,\pi_{dpn}\}$, the service ratio(ρ) to calculate the number of coins to pay the service provider from P, the penalty price (σ) applied to DPs in the case of the luck of the commitment, the time when a DR requests the creation of the SC (trequest), the time when the SCis effectively created (creationtime), the time when the data trading operation is completed (tdt), and the closing time of the SC (closetime). In addition, to protect against malicious DR and DPs, the DR and each DP should move a deposit from their wallet addresses to the contract address. Specifically, the DR and DPs should move numbers of coins to ($deposit_{dr}$) and $\{deposit_{dp1},...,deposit_{dpn}\}$ respectively. Figure 44 describes the implementation of the SC. The data trading SC consists of one public function, which can be called by vehicles, and four private functions, which can only locally be called by the BS.



```
Algorithm 1: Secure Data Trading Smart Contract
1  State variables:;
2    $SC\_address$, $ID_{dr}$, $\{ID_{dp_1},..., ID_{dp_n}\}$, $account_{dr}$;
3    $\{q_{dp_1},..., q_{dp_n}\}$, $\{account_{dp_1}..., account_{dp_n}\}$, $\mathbb{R}_{dr}$;
4    $\{\pi_{dp_1},..., \pi_{dp_n}\}$, $\mathbb{P}$, $\rho$, $\sigma$, $t_{dt}$, $creation\_time$;
5    $\{deposit_{dp_1},..., deposit_{dp_n}\}$, $Rep_{dr}$, $close\_time$;
6    $\{Rep_{dp_1},..., Rep_{dp_n}\}$, $deposit_{dr}$, $trequest$;
7
9  public Create()
10     Input: $Req^{dr \rightarrow sdnc_b}$;
11     if $(Rep_{dr} > 0)$ and $(balance_{dr} >= p\ (1 + (\frac{\rho}{Rep_{dr}}))$
        then
12         $SC\_address \leftarrow H(K_{dr} \,||\, ts)$ ;
13         $ID_{dr} \leftarrow K_{dr}$ ; $account_{dr} \leftarrow addr_{dr}$;
14         $deposit_{dr} \leftarrow$ Move$(balance_{dr}, p)$;
15         $\mathbb{P} \leftarrow p$ ; $\sigma \leftarrow p$ ; $trequest \leftarrow ts$, $\mathbb{R} \leftarrow$ R;
16     else
17         $Rep_{dr} \leftarrow (Rep_{dr}$ - 0.1) ; $Consensus()$ ;
18     end
20 private Negotiate()
21     Input: { $Mes^{v_1 \rightarrow sdnc_b}$,..., $Mes^{v_m \rightarrow sdnc_b}$ } ;
22     $\{dp_1,..., dp_n\} \leftarrow$ GT-Model$(\{q_{v_1},..., q_{v_m}\}, \mathbb{P})$ ;
23     $\{\pi_{dp_1},...,\pi_{dp_n}\} \leftarrow \frac{q_{dp_i}}{\sum_{j=1}^{n} q_{dp_j}} \mathbb{P}^*$;
24     $\forall\ dp_i \in \{dp_1,..., dp_n\}$ : Send $(Mes^{sdnc_b \rightarrow dp_i}(\pi_{dp_i},\sigma))$ ;
26 private Deploy()
27     Input:
28     for $dp_i \in \{dp_1,..., dp_n\}$ do
29         if $(balance_{dp_i} > 0)$ then
30             $ID_{dp_i} \leftarrow K_{dp_i}$ ; $account_{dp_i} \leftarrow addr_{dp_i}$;
31             if $(balance_{dp_i} >= \sigma\ )$ then
32                 $deposit_{dp_i} \leftarrow$ Move$(balance_{dp_i}, \sigma)$;
33                 $Rep_{dp_i} \leftarrow (Rep_{dp_i} + 0.1)$;
34             else
35                 $deposit_{dp_i} \leftarrow$ Move$(balance_{dp_i})$;
36                 $Rep_{dp_i} \leftarrow (Rep_{dp_i} + 0.05)$;
37             end
38         end
39     end
40     if $Consensus()==true$ then
41         $creation\_time \leftarrow timestamp$ ;
42         Send $(Conf^{sdnc_b \rightarrow dr})$;
43         $\forall\ v_i \in \{dp_1,..., dp_n\}$: Send $(Conf^{sdnc_b \rightarrow v_i}())$;
44     end
46 private Invoke()
47     Input: $Msg^{dr \rightarrow sdnc_b}$ ;
48     $t_{td} \leftarrow timestamp$ ;
49     Update $(\{l_{dp_1}, ...., l_{dp_n}\})$ ; $Consensus()$;
50     $Execute\_contract()$ ; $Close()$;
52 private close()
53     $close\_time \leftarrow timestamp$ ; $Consensus()$;
```

Figure 44: Secure Data Trading Smart Contract

1) Create

This function is called each time a vehicle vi(DR) requests for data. Thus, DR sends a request ($Req^{dr\text{--}\rightarrow sndcb}$) to (sndck) via the nearest bsj. We denote (sdncb) the (sndck) receiving the DR's request. $Req^{dr\text{--}\rightarrow sdncb}$ = EPK_{sdncb} ($addr_{dr}$ || p || R || Kdr ||Sig_{Kdr}|| $Cert_{Kdr}$||ts). This request is encrypted by PKs_{dncb} and includes the DR's account address ($addr_{dr}$), the maximum price (p) that DR can pay to perform this operation, the set of data requirements (R), DR's current pseudonym (K_{dr}), the corresponding signature(Sig(K_{dr})), certificate ($Cert_{Kdr}$), and timestamp ts. Once sdncb receives a request from a DR, it first checks Rep_{dr} and $balance_{dr}$ to verify if its reputation is positive and it has enough coins to pay for DPs and the service costs in step (11). The service costs are calculated as a function of the service rate pand the reputation value of the vehicle (Rep_{dr}). The higher the value of Rep_{dr}, the lower the cost of the service. If the condition is satisfied, the SCis created and a unique identifier is assigned to the $contract_{addres}$s in step (12), which consists of the hash value of the concatenation of the timestamp and the current pseudonym of the DR. The state variables (ID_{dr} and $account_{dr}$) related to the DR are also initialized in steps (13) and a deposit of p coins is moved from balance$_{dr}$ to deposit$_{dr}$ in step (14).P,R,σ, and t request are initialized in step (15). However, if the DR tries to execute a data trading operation without having enough coins in its balance, the request is refused, and the reputation value of the DR is decreased in step (17). A consensus process should also be done latter to update the blockchain ledger.

2) Negotiate

After creating the SC, a set of DPs should be selected to provide data to the DR. For this reason, (sdncb) analyses the data requirements (R) to determine the location of the requested data and select SDN controllers domains to which the request should be broadcast. Once the domains are selected, the request is broadcast to the corresponding SDNCs. These SDNCs are responsible for broadcasting the request to vehicles within their control zones via BSs and invite them to submit their data offers. Each vehicle that receives this request checks the data requirement; If a vehicle vi can satisfy the data requirement, it sends its data offer to sdncb via the nearest bsj: $Mes^{vi-\rightarrow sdncb}$= EPK_{sdncb} (q_{vi} || $addr_{dp}$ || $K_v i$ || $Sig_{Kv}i$ || $Cert_{Kvi}$ ||ts). This message is encrypted by PK_{sdnb} and includes q_{vi}, which is the quantity of data that a vehicle can provide. Here the DP is rational to decide the contribution level in terms of the amount of data to serve the DR. It also includes vi's account address ($addr_{dp}$), vi's current pseudonym (Kvi), the corresponding signature (Sig_{Kvi}), certificate($Cert_{Kvi}$), and timestamp (ts). In step 22, once all data offers are received by sdncb, it selects the best n vehicles {dp1,...,dpn} to act as DPs based on a game-theoretic model described in Section 3.1.6.4 . The game-theoretic model ensures the selection of DPs in the limit of the price provided by DR and provides the maximum utilities for the DR and DPs. If the price offered by the DR is not enough to pay for the DPs, sdncb sends a request to the DR mentioning the price(R^*) that should pay for the data trading operation. If the DR refuses the request of sdncb, the SC will be marked as closed. After selecting DPs, sdncb calculates the number of coins to pay for each DP {π_{dp1},...,π_{dpn}} in step 23. In step (24), once of the calculation of the payments of DPs is done, sdncb sends a message to each DP: $Mes^{sdncb-\rightarrow dpi}$=$EK_{dpi}$ (π_{dpi} || σ ||$Sig_{PKsdncb}$||ts). This message is encrypted by the current DP's pseudonym (Kdpi) and includes the number of coins (π_{dpi}), which the DP will receive after providing data, the penalty price(σ) applied to the vehicle in case of no respect of SC's clauses, and the signature (Sig_{PKsdnc}j)and the timestamp ts.

3) Deploy

Before deploying the SC into the consortium blockchain, sdncb checks the balance of each DP in step (29). If the balance is positive, the vehicle assigned as an DP and its related parameters (ID_{dpi}, $account_{dpi}$) are initialized in step (30). In addition, in step (31),sdncb checks if the vehicle has enough coins to pay for the penalty σ (if applicable). If the check passes, then a deposit of σ coins is moved from the DP's balance to the contract address in step(32) and the vehicle's reputation is increased by 0.1 in step(33). Otherwise, existing coins in the vehicle's balance are moved to the contract address in step (35) but the vehicle's reputation is increased by only 0.05 in step (35). In this stage, the SC is ready to be deployed into the blockchain. After reaching consensus in the consortium blockchain, the SC is successfully deployed and can be accessed by all the blockchain nodes. Once the SC is deployed, sdncb sets creation time in step (41). Then, it sends a confirmation message to the DR : $Conf^{sdncb-\rightarrow dr}$= EK_{dr}($Contract_{address}$|| $SigPK_{sdncb}$|| ts) in step(42). A confirmation is also sent to each DP {dp1,...,dpn} in step (43): $Conf^{sdncb-\rightarrow dpi}$=$EK_{dp}$i($Contract_{address}$||$\pi_{dpi}$||$Sig_{PKsndcb}$|| ts). The confirmation messages include the contract address ($Contract_{address}$), the signature $Sig_{PKsdncb}$ and the timestamp ts.

4) Invoke

After deploying the SC, each dpi uploads its data to the closest fog station and sends a message tosdncb:$Mes^{vi-\rightarrow sdncb}$= EPK_{sdnb} (q_{dpi} || fogid || K_{dpi}|| Sig_{Kdp}i || $Cert_{Kdpi}$ || ts). This message is encrypted by PK_{sdnb} and includes q_{dpi}, the quantity of data that dpi uploads to the fog station, and the identification of the fog station fogid. It also includes dpi's current pseudonym (Kdpi), the corresponding signature (Sig_{Kdpi}), certificate ($Cert_{Kdpi}$), and timestamp (ts). The fog station also checks the quantity and the quality of data provided by the DP and send the feedback to sdncb: $Fd^{fog-\rightarrow sdncb}$. Once all the requested data are uploaded to fog stations, sdncb sends a command to concerned SDNCs to migrate data to a fog node closest to the DR. Once the data migration is done, the DR sends a message $Conf^{sdncb\text{–}\rightarrow dr}$ to the DR to download it. $Conf^{sdncb\text{–}\rightarrow dr}$= EK_{dr} (fogid || $Sig_{PKsdncb}$|| ts). This message is encrypted the DR's pseudonym and includes the fog ID_{fogid}, the signature $Sig_{PKsdncb}$ and the timestamp ts. Once the all data are downloaded, the DR send a confirmation to sdncb: ($^{Confdr\text{–}\rightarrow sdncb}$). Once sdncb receives the confirmation message, it set t_{td} in step (48) and update the quality of data provided by DPs and updated in the ledger in step (49). Then, it executes the SC is in step (49). Thus, the financial transactions concerning payments and penalties are generated and prepared for block building. The penalty is applied to every dpi that doesn't provide the quality of data expressed in its data offer. Finally, the function Close() is called for running the consensus progress and closing the smart contact.

5) Close

This function starts by deactivating all the functions of the smart contract and assigning the close time (closetime). Then, a consensus process is executed in step (53) to update the ledger, as described in the next section.

B. Utility-based Delegated Byzantine Fault Tolerance Consensus Protocol

To ensure that a coherent and recognized for all members of the blockchain, we propose high scalability enabled consensus protocol called the Utility-based Delegated Byzantine Fault Tolerance (U-DBFT) consensus protocol, which is based on Krauß et al. (1997). Our consensus protocol comprises two steps: (i) the selection of the leader and consensus members, and (ii) the consensus process.

1) Consensus members and leader selection

The members of the consortium blockchain (SDNCs) have two types of roles: (i) simple members that can only broadcast transactions into the blockchain network and accept the validated blocks, and (ii) consensus members: can participate in consensus processes. In our scheme, the selection of the consensus members depends on their utility values{ U_{sdnc1}, ...U_{sdncn}}, which are computed according to the scores received from data trading participants. Thus, the top (M) SDNCs with the highest utility values are selected as consensus members as shown in formula 33.

$$\{sdnc_1, ...sdnc_{\mathbb{M}}\} = Max(\{U_{sdnc_1}, ..., U_{sdnc_n}\}, \mathbb{M})$$

Formula 33

We denote M the set of consensus members. We assume that M>= 3f+1, where f is the maximum number of malicious members in the consortium blockchain. As shown in formula 34, the utility of a sdnck (U_{sdnck}) is the average of the sum of scores of data trading participant weighted by their reputation values given after the data trading operation

$$U_{sdnc_k} = \frac{1}{nb_{sco_{dr}}} * \sum_{i=1}^{nb_{sco_{dr}}} (Rep_{dr_i} * Score_{dr_i}) + \frac{1}{nb_{sco_{dp}}} * \sum_{j=1}^{nb_{sco_{dp}}} (Rep_{dp_j} * Score_{dp_j})$$

Formula 34

nb_{scodr} and nb_{scodp} are the number of scores received from the DR and DPs, respectively. $Score_{idr}$ is the score given by adritosdnck, which is calculated using formula 35.

$$Score_{dr} = \frac{\sum_{i=1}^{nb1_{dt}} (lu_{dr_i} + cs_i + ps_i)}{nb_{dt}}$$

Formula 35

$nb1_{dt}$ is the number of data trading operations where the vehicle is involved as a DR. The score of an sdnck is calculated based on the average of the sum of values obtained after the date trading. These values are: (i) the local utility of dr(lu_{dr}) given by formula 42, as discussed in Section 3.4.6.4, (ii) the processing speed (ps) given by the formula 36, which assesses the speed of establishing the SC including the selection of the candidate vehicles and sending/receiving messages, and (ii) the consensus speed of the block(cs), given by the formula 37.

$$ps = \frac{max_{tp} - tp}{max_{tp}}$$

Formula 36

Where tp is the effective processing time, and max_{tp} is the maximum expected time for processing.

$$cs = \frac{max_{tc} - tc}{max_{tc}}$$

Formula 37

Where tc is the effective time for the consensus process and max tc is the maximum taken for the consensus process of one block.

On the other hand, $Score_{dp}$ is the score given by a dpi to sdnck. As shown in the formula 38, a dp calculates the score according to the average of the sum of: the local utility of dp (ludp), given by formula 38 as discussed in Section 3.4.6.4, cs (formula 37) and ps (formula 36) values obtained after each PCP. Here, $nb2_{dt}$ is the number of data trading operations where the vehicle is involved as a dp.

$$Score_{dp} = \frac{\sum_{i=1}^{nb_{dt}} (lu_{dp_i} + cs_i + ps_i)}{nb_{dt}}$$

Formula 38

To protect utility values from malicious SDNCs that aim to monopolize the consensus process through tampering utility values, we propose to store the utility values into the ledger. The scores of vehicles are broadcast to the blockchain. Each ΔT2, the utility values of SDNCs are calculated and a consensus process is carried out to update the set of the consensus members (M). In our scheme, the selection of the leader pi s done according to high utility descendent and following around-robin (circular) policy using the formula 39.

$$p = v \ mod \ \Omega$$

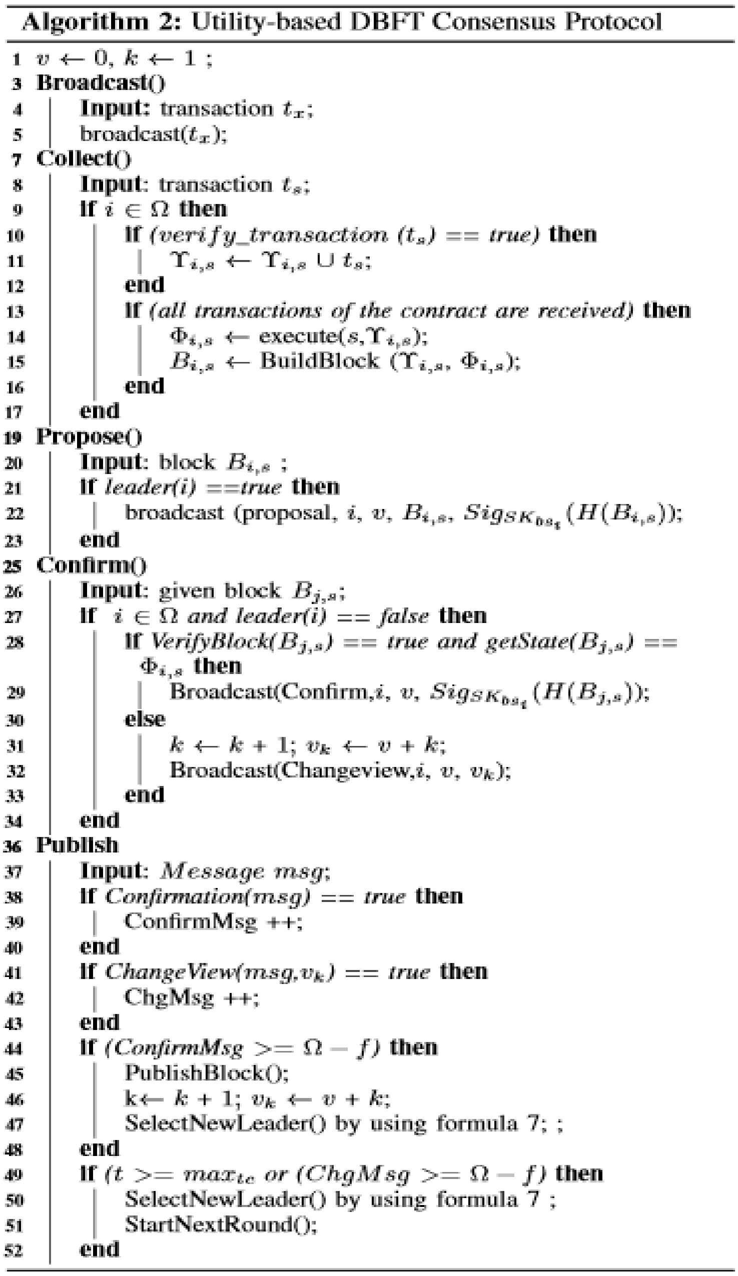
Formula 39

Based on Krauß et al. (1997), a view v is a period of time in which a given consortium member is the leader. In formula 39, vis an identifier of a given period of time. Therefore, a view change means switching to a different leader.

2) Consensus process

Figure 45 describes the consensus process runs by a consensus member(i) for transactions and states related to a SC. However, the same consensus process is applied to the blocks related to the reputation, data quality and utility values. Here ts is a transaction record related to the SC, $Y_{i,s}$ is a set of SC's transactions validated by the consensus member i.Φi,sis the updated state after the execution of SC with the set of corresponded transactions $Y_{s.Bi}$ is a local block created by the consensus member i, verifytransaction(ts) is a function to the verify the validity of a transactionts,execute (Yi,s)is a function that locally executes the SC with the corresponded transactions Yi,s, BuildBlock (Yi,s,Φi,s) is to build local block witht he transaction set Yi,s and the state set Φi,s. The consensus process then contains the following steps:

- **Broadcast:** When sdncb executes an SC between a DR and a set of DPs, it broadcasts all the corresponded transactions into the whole consortium blockchain for audit and verification.
- **Collect**: All of SC's transactions are collected by consensus members. In step (10), each transaction ts is verified, and only validated transactions are added to Yi,sin step (11). In step (14), each consensus member waits to receive all the SC's transactions before it locally executes the SC. After executing the SC, the changed states are saved in the local state ledger of each consensus member. All validated transactions and states are ordered by the timestamp and packaged into a block in step (15).
- **Propose**: In step (22), after all, non-leader consensus members have finished building their local blocks, the leader consensus member broadcasts a proposal to all non-leader consensus members. This proposal includes leader's identifier(i), the view v, the local block (Bi,s), and the hash value of the block (H(Bi,s)) singed by SK_{sdnci}.
- **Confirm:** Once a non-leader vehicle receives a candidate block Bj,s, it first verifies its validity using verify Block(), then it uses the function getState() to retrieve the state of the block for comparing it with its local state Φi,s. If the check passes, each non-leader consensus member broadcasts a confirmation message in step (29), which includes its identifier i, the view change v and the signature the hash of the block (Sig_{SKbsi}(H(Bj,s)). However, if the received block is not valid, the view change will be triggered, where the next view change vk is calculated in step (31). Therefore, the non-leaderconsensus member will broadcast the changeviewMsg message in step (32), which includes non-leader's identifier (i), the current view v, and the changed view vk.
- **Publish**: Each consensus member keeps counting the number of received confirmations and the number of views changes vk in steps (39) and (42) respectively. If the number of received confirmation messages is no less (ω−f) massages from other distinct consensus members ,the consensus is reached and the block is ready to be published in the blockchain. To ensure tractability and verification, each block is added in chronological order into the blockchain and includes a cryptographic hash to the prior block. To prepare for the next consensus process, the view is changed in step (46) and the next leader is selected in step (47) using the formula 7. However, if the max period to reach the consensus (max_{tc}) has passed or the number of received view change messages with the same vki s at least (Ω−f)from distinct consensus members, a new leader is selected in step (50) and the next round of the consensus process will start in step (51).



```
Algorithm 2: Utility-based DBFT Consensus Protocol
$v \leftarrow 0$, $k \leftarrow 1$ ;
Broadcast()
    Input: transaction $t_x$;
    broadcast($t_x$);
Collect()
    Input: transaction $t_s$;
    If $i \in \Omega$ then
        If $(verify\_transaction\ (t_s) == true)$ then
            $\Upsilon_{i,s} \leftarrow \Upsilon_{i,s} \cup t_s$;
        end
        If (all transactions of the contract are received) then
            $\Phi_{i,s} \leftarrow$ execute($s$,$\Upsilon_{i,s}$);
            $B_{i,s} \leftarrow$ BuildBlock ($\Upsilon_{i,s}$, $\Phi_{i,s}$);
        end
    end
Propose()
    Input: block $B_{i,s}$ ;
    If leader(i) ==true then
        broadcast (proposal, $i$, $v$, $B_{i,s}$, $Sig_{SK_{bs_i}}(H(B_{i,s}))$;
    end
Confirm()
    Input: given block $B_{j,s}$;
    If $i \in \Omega$ and leader(i) == false then
        If VerifyBlock($B_{j,s}$) == true and getState($B_{j,s}$) ==
          $\Phi_{i,s}$ then
            Broadcast(Confirm,$i$, $v$, $Sig_{SK_{bs_i}}(H(B_{j,s}))$;
        else
            $k \leftarrow k + 1$; $v_k \leftarrow v + k$;
            Broadcast(Changeview,$i$, $v$, $v_k$);
        end
    end
Publish
    Input: $Message\ msg$;
    If Confirmation(msg) == true then
        ConfirmMsg ++;
    end
    If ChangeView(msg,$v_k$) == true then
        ChgMsg ++;
    end
    If (ConfirmMsg >= $\Omega - f$) then
        PublishBlock();
        k$\leftarrow$ $k + 1$; $v_k \leftarrow v + k$;
        SelectNewLeader() by using formula 7; ;
    end
    If $(t >= max_{te}$ or $(ChgMsg >= \Omega - f)$ then
        SelectNewLeader() by using formula 7 ;
        StartNextRound();
    end
```

Figure 45: Utility-based DBFT Consensus Protocol

3.4.6.3 Fog Station Emplacement

The placement of fog stations relative to DPs and the DR is essential to provide low-latency data trading comprising data uploading and downloading. Leveraging SDN control plane, our scheme ensures dynamic and mobility-aware placement of fog stations over BSs. In this section, we formalize the fog placement problem as a linear programming model and subsequently propose an SDN-based genetic algorithm to solve it.

A. Problem formalization

We assume that m BSs exist on a zone controlled by an sdnck, with m>=N$_{fog}$, where N$_{fog}$ is the number of fog stations that are required to offer the data trading service on this geographic zone. Thus, the problem consists of finding the best BSs that should host fog stations at time t to reduce latency in transmitting/receiving data. The problem can be formulated as follows: Let i= {1,...,n} the set of existing vehicles in the zone at timet. Let j ={1,...,m} be the set of the candidate BSs to deploy fog stations. Let cij the delay that takes a vehicle vi to transmit/receive data to/from BSj. Since cij depends on the distance (dij) between a vehicle i and BS i, we consider dij instead of cij. Let yj a binary decision variable, which indicates that the BS is selected to host a fog station at time t. xij is a binary variable, which indicates that the vehicle vi is assigned to BSj or not. To select the best BSs to host fog stations, we should minimize the following objective function F (Formula 40). Specifically, F aims to minimize the delay of uploading/downloaded data to the assigned fog stations.

$$F = min \sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} x_{ij}$$

Formula 40

The feasibility of the solution depends on different constraints, which are represented by the following equations:

$$\begin{cases} \sum_{j=1}^{m} x_{ij} = 1 & \text{... (a)} \\ \sum_{j=1}^{m} y_j = N_{fog}(t) & \text{... (b)} \\ \sum_{j=1}^{n} x_{ij} * q_{ij} <= K_{fog} & \text{... (c)} \\ x_{ij} \in \{0,1\} & \text{... (d)} \\ y_j \in \{0,1\} & \text{... (e)} \end{cases}$$

Formula 41

(a) ensures that each vehicle vi is only assigned to one BS; (b) ensures that the number of selected BSs is equal to the number of fog stations that are needed at time t ($N_{fog(t)}$), which can be calculated based on the model proposed by Boualouache et al. in 2020 (c) guarantees that the sum of the amount of data of vehicles that are assigned to each BS does not exceed the storage capacity of the fog station (Kfog) (J. Zhang et al., 2019); and finally, (d) and (e) are the integrity constraints.

B. A Genetic Algorithm for an Optimal Placement of Fog stations

The fog station placement is a NP-hard problem. Hence, leveraging a meta-heuristic approach, we propose a Fog Station Placement Genetic Algorithm (FSPGA) for optimized placement of fog stations within BSs. The flowchart of this algorithm is illustrated in Figure 46. FSPGA runs son each SNDC and periodically takes as input the current mobility information of vehicles and the positions of BSs and returns the fog station placement decision. In the following, we describe the main steps of this algorithm.

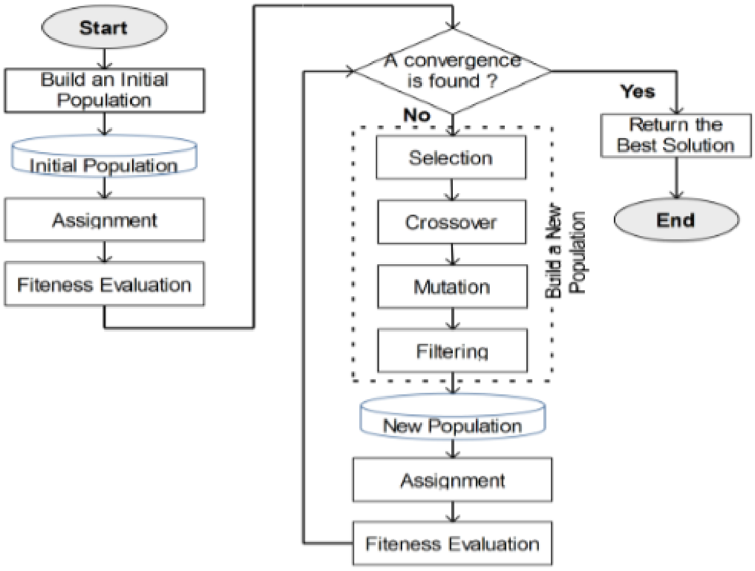


Figure 46: FSPGA flowchart

- **Initialisation Phase**: In this phase, the initial population of chromosomes is randomly generated, and vehicles are also assigned to each generated chromosome to compute the fittest chromosome. A chromosome is a chain of integers where each value is the index number of a potential BS. To avoid invalid chromosomes, FSPGA checks for each generated gene if it has already been added to the given chromosome or no. The random population procedure runs until the generation of all chromosomes.

- **Selection Phase**: In this phase, a set of chromosomes from the old population are selected to be parents for crossover and mutation phases. FSPGA uses two selection methods: elitism and tournament. FSPGA uses elitism to select the best fittest chromosome from the old population and adds them to the new population. FSPGA also uses the tournament method to select the parents that are used by the crossover to generate new chromosomes. The tournament selection method randomly chooses a set of chromosomes from the old population. After that, the fitness of each tournament chromosome is evaluated, and the fittest chromosome is selected as a parent for the crossover.
- **Crossover Phase**: Crossover selects genes from the selected parents to create the new chromosome. The crossover runs until the generation of the new population. In each iteration, a new chromosome is created based on the two-parent chromosomes, which were selected using the tournament selection method. The genes of the new chromosome are copied either from the first or the second parent according to a crossover probability.
- **Mutation Phase**: The mutation operator works on a single chromosome. It aims to randomly introduce a new gene instead of inheriting it from the old chromosomes. The mutation runs until the generation of the new population. In each iteration, the genes of each chromosome are changed according to the mutation probability. In case a change is needed, a gene is randomly generated from the whole search space.
- **Assignment Phase**: The assignment of vehicles to genes (BSs) of each chromosome is needed to evaluate the fitness. FSPGA calculates the Euclidean distances between each vehicle vi and each candidate BSj. These distances are saved in the distance table, which is sorted from the lowest to the highest distance value. Then each vehicle is assigned to the nearest BS and save this assignment in this table.
- **Fitness evaluation**: Each generation of the genetic programming approach goes through mutations and crossovers. The newly generated solutions are evaluated according to a fitness function. We derive the fitness function according to the objective function (Formula 36).
- **Stop conditions**: FPGA considers two stop-conditions related to two different aspects: (i) the convergence of our solution: if the fitness value keeps unchanged during three iterations, and (ii) the number of iterations. We have simply limited the maximum number of iterations. FSPGA returns the fittest chromosome (i.e., the chromosome with minimal fitness value).

3.4.6.4 Vehicular Data Trading Stackelberg Game

In this section, we formulate the vehicular data trading process as a Stackelberg game based on Zhang et al. (2019). This game consists of the DR acting as the leader and several DPs acting as followers. We also apply the backward induction method to solve the Stackelberg equilibrium, which ensures the maximum utility for game participants.

A. Problem Formulation

We assume that a data trading process is performing between a given a DR (dr) and a set of n DPs D ={dp1,dp2,.....,dpn}, where sdncb is acting as a broker between the DR and the set of DPs. Each dpiis rational and independently decide the level of contribution in terms of the amount of data $q_{dp}i$ to serve the DR. To ensure fair data trading, the reward that each dpi gets is proportional with the amount of data q_{dpi} in the total data required by the DR. In addition, the utility of dpi does not only depend on the reward it gets for providing data but also the energy consumption and the processing overhead. Indeed, DPs need to consume a certain amount of energy to collect and upload data. Let αi represent the amount of consumed energy per unit size, thus the overall energy consumption for d_{pi} is α_i $q_{dpi.}$ Moreover, due to the resource limitation of vehicles, data trading generates additional processing overhead, may cause unnecessary inconvenience to different processes running on dpi.

We formulate this processing overhead as β q_{dpi}^2, where β is the processing overhead factor (Huang et al. 2018). To this end, the utility function of dpi is given by formula 42.

$$u_{dp_i} = \frac{q_{dp_i}}{\sum_{j=1}^{N} q_{dp_j}} \mathbb{P} - \alpha_i q_{dp_i} - \beta q_{dp_i}^2$$

Formula 42

$\sum_{i=1}^{N} l_i q_{dp_i}$ where ℙ is the price set by the dr for the data trading process. On the other hand, the utility function of the dr (U_{dr}) depends on the monetary costs it pays (ℙ) and the quality of data that it obtains. Thus, the utility gain of the dr is related to the total amount of q_{dp}i with corresponding data quality level l_i simultaneously, which is denoted by To this end, U_{dr} is given by formula 43.

$$U_{dr} = \sum_{j=1}^{N} l_j q_{dp_j} - \mathbb{P}$$

Formula 43

B. Analysis of Stackelberg Equilibrium

The data trading problem between the (dr) and N DPs is formulated as a typical Stackelberg game. The DR (dr) acts as a leader, while N DPs are regarded as followers. For motivating the DPs to participate in data trading, the dr stimulates all the DPs with reward parameter ℙ. According to the given reward parameter ℙ, the DPs determine the amount of data to provide (q_{dpi}) for maximizing their utilities. In our scheme, we assume that sdncb can be fully aware of the strategies and actions of DPs. Thus, DR can be replaced with a broker sdnb to determine the optimal reward parameter ℙ*. For a given reward ℙ*, each DP decides the best response q^*_{dpi} to maximize the payoffs. The goal of the proposed game is to find the unique Stackelberg equilibrium, where both the DR and DPs have no motivations to change their strategies unilaterally (Zhang 2009). The Stackelberg equilibrium is defined as follows.

Definition 1: we consider a series of decisions (q^*_{dpi},P*)as the Stackelberg equilibrium, when and only when it meets the following set of inequalities (formula 44).

$$\forall q_{dp_j}, u_{dp_j}(q_{dp_j}^*, \mathbb{P}^*) \geq u_{dp_j}(q_{dp_j}, \mathbb{P}^*)$$
$$\forall \mathbb{P}, U_{dr}(q_{dp_i}^*, \mathbb{P}^*) \geq U_{dr}(q_{dp_i}^*, \mathbb{P})$$

Formula 44

First, we analyse the optimal strategy of a DP. The second derivative of u_{dpi} is given by formula 45.

$$\frac{\partial^2 u_{dp_i}}{\partial q_{dp_i}^2} = -2\frac{\sum_{j \in D, j \neq i}^{N} q_{dp_j} \sum_{j=1}^{N} q_{dp_j}}{\left(\sum_{j=1}^{N} q_{dp_j}\right)^4} \mathbb{P} - 2\beta < 0$$

Formula 45

$\frac{\partial^2 u_{dp_i}}{\partial q_{dp_i}^2} < 0$, so u_{dpi} is concave, so the maximal value of u_{dpi} must exist. The first-order optimally condition $\partial u_{dpi}/\partial q_{dpi}= 0$ is given by formula 46:

$$\frac{\sum_{j=1}^{N} q_{dp_j} - q_{dp_i}}{\left(\sum_{j=1}^{N} q_{dp_j}\right)^2}\mathbb{P} - \alpha_i - 2\beta q_{dp_i} = 0$$

Formula 46

Adding up formula 41 over N DPs and solving the equations to find $\sum_{j=1}^{N} q_{dp_j}$. Then, once $\sum_{j=1}^{N} q_{dp_j}$ calculated is substituted in formula 46, to find the best response of $q_{dpi}(q^*_{dpi})$, which is given by formula 47 (more information can be found at (Huang et al., 2018).

$$q^*_{dp_i} = \frac{\mathbb{P}(\omega\sqrt{f + r\mathbb{P}} + \theta) - \alpha_i(\omega\sqrt{f + r\mathbb{P}} + \theta)^2}{R + 2\beta(\omega\sqrt{f + r\mathbb{P}} + \omega)^2}$$

Formula 47

Where ω= 1/4β, r= 2 (N-1) / f =$^{\theta\ =\ -\omega\ \sum_{j=1}^{N}\alpha_j,}$ is the optimal strategy of dpi in determining the amount of data to provide to the dr, which maximizes individual utility considering the reward value P. On the other hand, to demonstrate the impact of the data level on $\left(\sum_{j=1}^{N}\alpha_j\right)^2$ is the optimal strategy of dpi in determining the amount of data to provide to the dr, which maximizes individual utility considering the reward value P. On the other hand, to demonstrate the impact of the data level on U_{dr} we consider $\sum_{j=1}^{N} l_j q_{dp_j}$ the overall data level of DPs¯l instead of the data level of each dp. Therefore, it is replaced with¯l∑Nj=1qdpj. Udr is then given by formula 48.

$$U_{dr} = \bar{l}\sum_{j=1}^{N} q_{dp_j} - \mathbb{P}$$

Formula 48

By substituting formula$\sum_{j=1}^{N} q_{dp_j}$, which is found solving formula 46, we can get formula 49.

$$U_{dr} = \bar{l}(\omega\sqrt{f + r\mathbb{P}} + \theta) - \mathbb{P}$$

Formula 49

The second derivative of U_{dr} is given by formula 50.

$$\frac{\partial^2 U_{dr}}{\partial \mathbb{P}^2} = -\frac{\omega r^2 \bar{g}}{4}(f + r\mathbb{P})^{-\frac{3}{2}} < 0$$

Formula 50

$\frac{\partial^2 U_{dr}}{\partial \mathbb{P}^2} < 0,$ so U_{dr} is concave, so the maximal value of U_{dr} must exist. The first-order optimally condition$\partial U_{dr}/\partial P = 0$ is given by formula 51

$$\frac{\omega r\bar{l}}{2}(f + r\mathbb{P})^{-\frac{1}{2}} = 1$$

Formula 51

After solving the formula 46, we obtain the optimal strategy P^* as follows (formula 52),

$$\mathbb{P}^* = \frac{\bar{l}^2(N-1)^2 - (\sum_{i=1}^{N} \alpha_i)^2}{8\beta(N-1)}$$

Formula 52

Theorem: There exists the unique Stackelberg equilibrium between the DR and all participant DPs in our proposed Stackelberg game.

Proof: As proven by formula 40, in the response of a given reward parameter P, each DP has its unique optimal strategy q^*_{dpi}. In addition, since sdnb has full knowledge of all the best responses of $\forall d_{pi} \in D$, q^*_{dpi}, the utility function of the DR can be adjusted accordingly. The maximum utility of the DR, P^* can be found using the formula 52, which is the best strategy given the optimal responses from all DPs, with $\partial 2U_{dr}/\partial P^2<0$. To this end, both the leader and followers are satisfied with their decisions $(q^*_{i,v},P^*)$ and have no motivation to change their strategies. Thus, the unique Stackelberg equilibrium is reached in this game.

3.4.6.5 Performance Evaluation

This section evaluates the performance of our scheme. We first evaluate consensus time considering Luxembourg as a study case. We then perform an equilibrium analysis of the vehicular data trading game. Finally, we evaluate fog placement time considering the number of fog stations and vehicular density as parameters.

A. Blockchain analysis

In this section, we perform analytic evaluations on the consensus time in the consortium blockchain enabling vehicular data trading

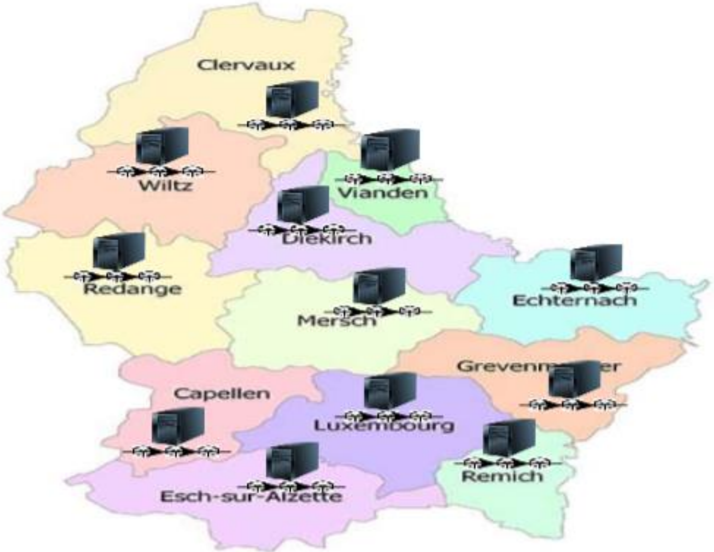


Figure 47: A case study of vehicular data trading in Luxembourg

Figure 47 shows the map of Luxembourg. The country consists of 12 cantons and is one of the first countries which start deploying 5G in 2020. We consider that each canton is controlled by one SDNC. We first evaluate the average time to reach the consensus considering different numbers of consensus members. For this reason, we run a python implementation of the DBFT consensus protocol in a machine equipped with a CPU (Intel i5 2.6 GHz) and 8 GB of RAM.

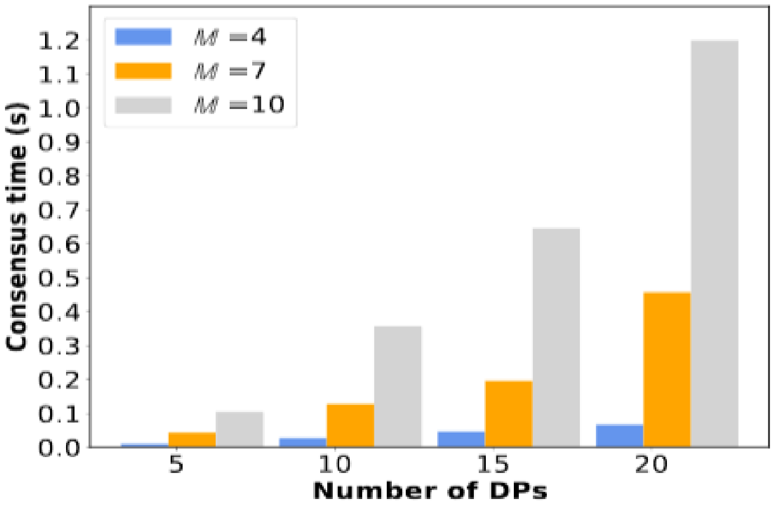


Figure 48: The consensus time for a data trading process with the variation of the number DPs and the number of consensus members

Figure 48 illustrates the consensus time for one vehicular data trading process. We consider different numbers of DPs∈ {5,10,15,20}, which equals the number of transactions generated after the SC's execution. We also consider different consensus members M∈ {4,7,10}. The results show the consensus time increases with the number DPs and M, respectively. However, only a short time is needed to reach a consensus. Indeed, a consensus process with 20 DPs with 4 consensus members takes only 1.2s. It is worth noting that the consensus time is the time required for a block to be inserted in the blockchain, which has no impact on road safety. In the second evaluation, we consider a large-scale study case where the DRs are located in Luxembourg city while the DPs are located in other cantons. Luxembourg city counts around 288 thousand vehicles circulating in the city over 24 hours (Codeć et al. 2017). During the peak hour (high density) more than 4.7 thousand vehicles can be found on roads, while at midnight (low density), only 700 vehicles can be found on roads. In Figure 49, we estimate the consensus time under low and high vehicular densities scenarios while considering different probabilities to request for data trading from vehicles. Our evaluation considers that the maximum number of vehicles that can request data at the same time is 20%. In addition, we consider 10 DPs are involved in each vehicular data trading process and 4 out of 12 SDNCs are consensus members. Figure 49 shows that the consensus time increases with the vehicular density and the probability of request, respectively. However, that the consensus time remains short (less than 3s).

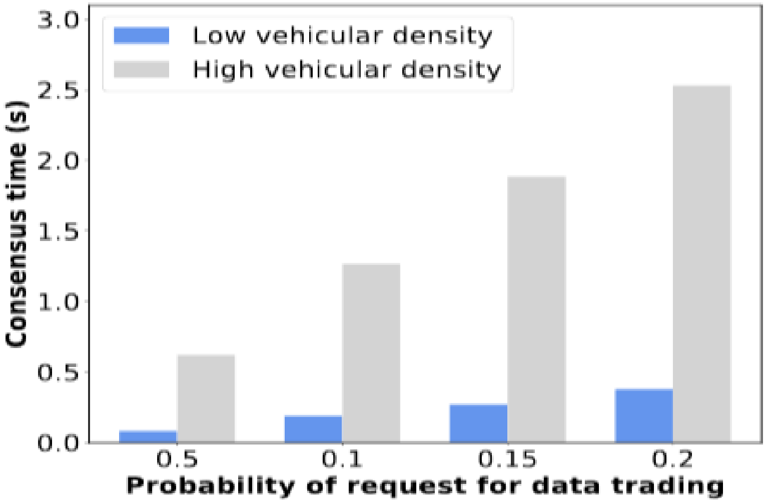


Figure 49: The consensus time considering low and high vehicular densities with the variation of the probability of request for data trading (M= 4)

B. Vehicular data trading game analysis

In this section, we analyze the Stackelberg data trading model. Specifically, we analyze the best responses of the DR and DPs considering different model parameters. In this evaluation, we consider that the vehicular data trading process consists of 10 DPs. We also consider that the model parameters α and β are in the range [0.1−0.9]. In addition, we assume that P ∈ [1−100]. In Figure 50, we evaluate the utility U_{dr} varying P and ̄l. As we can see in Figure 50, U_{dr} is influenced by different price values P. In addition, U_{dr} increases with the data quality level *l*. The dashed lines in Figure 50 also shows the best strategy of DR P^* to have the maximum utility for each data quality level l. Thus, the DR should increase its P^* for encouraging DPs to provide higher data quality levels. For example, to increase the data quality level l from 1.5 to 1.8, the DR should increase the value of P^* from 20.06 to 26.95 .i.e. 34%.

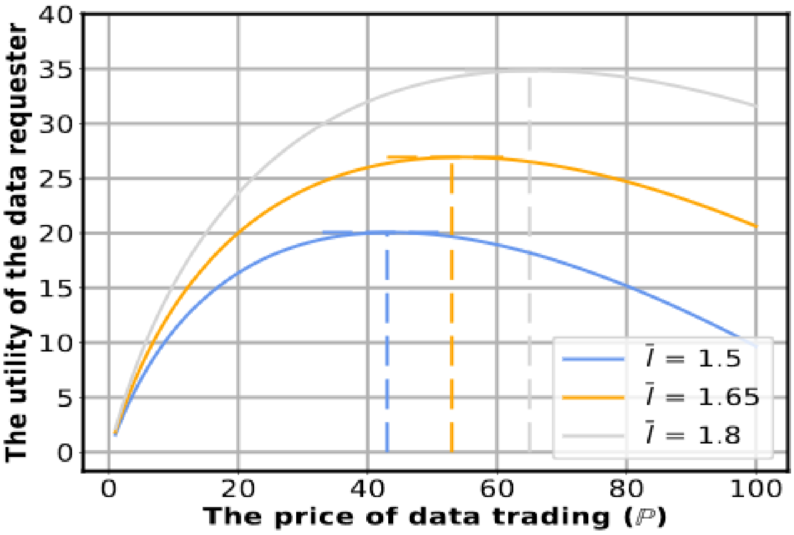


Figure 50: The utility of the DR with the variation P and l

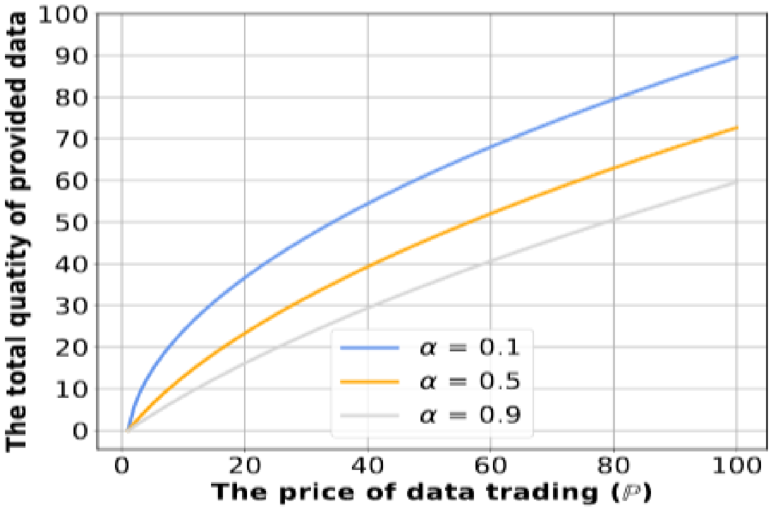


Figure 51: The amount of data provided by DPs with the variation of α

On the other hand, the total amount of data provided by DPs is not influenced by P* but also by the consumed energy parameter α and the processing overhead factor β. In Figure 51, we estimate the total amount of data provided by DPs with the variation of α within the same range of P. Three values of α were considered {0.1,0.5,0.9}. Higher values of αmeans that DPs consume more energy to provide. Consequently, DPs prefer to decrease the provided amounts of data with the same given P. For example, if we assume that P= 60 and increases the value of α from 0.1 to 0.5, the total amount of provided data decreases from 68.04 to 52.03, i.e., 23%. Similarly, in Figure 52, we estimate the total amount of data with the variation of β within the same range of P. As we can see, at the higher value of β, the DPs also reduce their amounts of provided data.

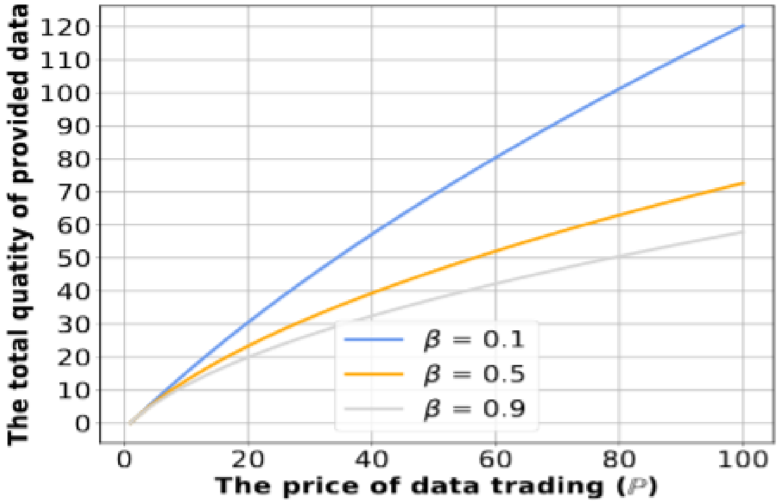
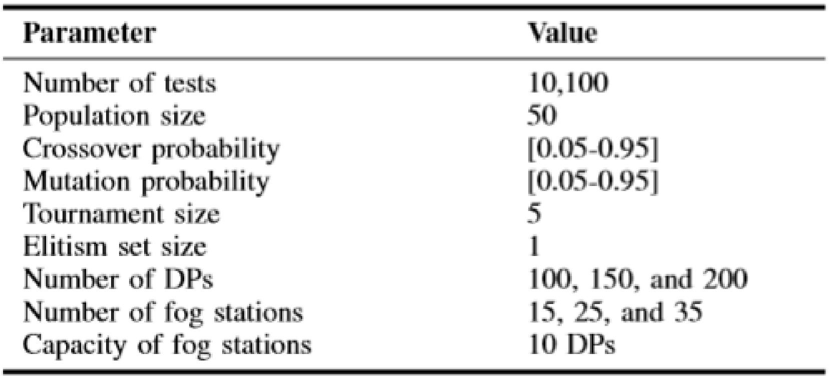


Figure 52: The amount of data provided by DPs with the variation of β

C. Fog placement analysis

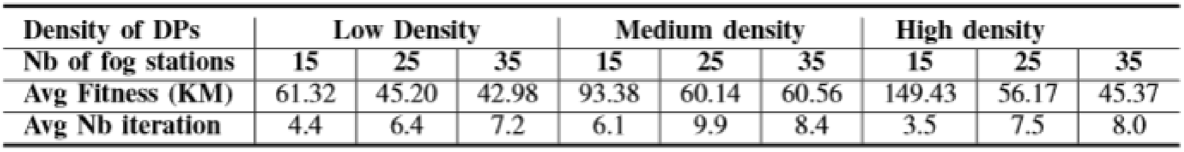
In this section, we evaluate the performance of FSPGA. In this evaluation, we consider that DPs are located in Luxembourg City. The SDNC aims to place the fog stations near DPs to provide a collection of DATA. We three levels of DPs Density: Low, Medium, and High for 100, 150, and 200 DPs. The area of Luxembourg is 100KM^2 and around 150 base stations are deployed in the city. We also varied the number of fog stations from 15 to 35. We consider that storage capacity of each fog station can store data for 10 DPs. FSPGA is programmed and implemented using Java programming language and run on Intel i5 2.6 GHz. Table 22 shows the parameters used by FSPGA. We set the size of the generated population in each iteration to 50. We fixed the tournament size and the elitism parameters to 5 and 1, respectively and the crossover probability and the mutation probability to 5%to 95%, respectively. Each test is repeated 10 times and the results are calculated with 95% of the confidence interval.



Parameter	Value
Number of tests	10,100
Population size	50
Crossover probability	[0.05-0.95]
Mutation probability	[0.05-0.95]
Tournament size	5
Elitism set size	1
Number of DPs	100, 150, and 200
Number of fog stations	15, 25, and 35
Capacity of fog stations	10 DPs

Table 22: Simulation Parameters

In Table 22, We evaluate the fitness and the convergence speed obtained under different DPs densities. As we can see, the fitness decreases with the increase in the number of fog stations for all DPs densities. For Low and Medium densities, the fitness values approximately keep stable values between 25 and 35 fog stations. However, for high densities, the value of fitness is enhanced in this interval. The reason for that with a high density of vehicles and with a large number of fog stations, the distances between the DPs and fog stations will be short. As a result, the fitness value decreased. Table 23 also illustrates the speed convergence under different DPs densities. We notice that the number of iterations increases with the number of fog stations for all DPs densities. In addition, the convergence speeds of DPs densities are close when the number of fog stations equals to 35. These results can be explained that with a large number of fog stations, the search space of FSPGA will be larger. Consequently, FSPGA takes more iterations to reach the fittest chromosome, whatever the DPs densities are. To run adequately, FSPGA needs an accurate input such as the number of fog stations densities of the traffic, coordinates of DPs, etc. This input is provided by the SDNC, which supervises the behavior of the moving DPs via transmitted beacons and gets information about the fog stations. When a change occurs in the network, the SDN knowledge is updated. Going further, we have compared the performances of our scheme in terms of the response time of SDNC under different DPs densities. The response time is the time taken by the SDNC to select the placement of the fog stations. As shown in Figure 53, the response time increases with DPs density. The maximal value is 7 seconds which is observed under the high-density scenario.



Density of DPs	Low Density			Medium density			High density		
Nb of fog stations	15	25	35	15	25	35	15	25	35
Avg Fitness (KM)	61.32	45.20	42.98	93.38	60.14	60.56	149.43	56.17	45.37
Avg Nb iteration	4.4	6.4	7.2	6.1	9.9	8.4	3.5	7.5	8.0

Table 23: The fitness and the convergence speed obtained under different DPs densities

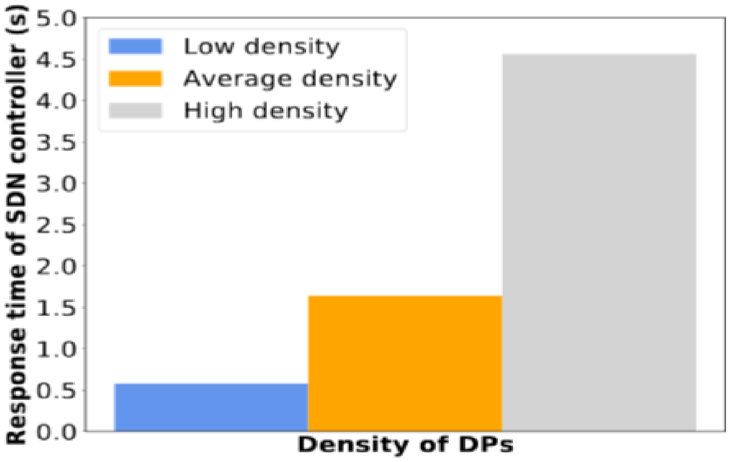


Figure 53: Response time of the SDN controller under different DPs densities

3.4.6.6 Discussion

In this section, we provide a short discussion on the features of our scheme in terms of scalability, security, privacy, fairness, and flexibility. Our scheme is scalable thanks to the hierarchical structure of our architecture. Indeed, each SDNC controls a limited region that includes a set of BSs/fog stations, which allows handling the mobility of many vehicles. In addition, our blockchain analysis shows a short consensus time process even with a large number of vehicles requesting data trading at the same time. On the other hand, our scheme provides a set of security checks to thwart attackers. For thwarting malicious DRs, a balance verification is performed for each requested data trading operation. Data trading operations are refused, and penalties are applied if DRs violate any SC clause. Similarly, for malicious DPs, penalties and reputation decreases are applied to DPs in the case of non-respect of SC clauses. Our scheme is also thwarting malicious SDNCs trying to tamper data since all relevant data such as reputation values, scores, and utility values in the blockchain. Moreover, privacy preservation is ensured by our scheme since pseudonyms are used instead of real identifiers as sources of transactions and as account addresses as well. Besides the features of SDN combined with a genetic algorithm, our scheme provides a dynamic and optimal placement of fog stations, which efficiently handle the mobility of vehicles and reduce the latency in vehicular data trading. Furthermore, SDNCs are acting as dealers between DRs and DPs to encourage DPs to provide high-quality data while offering fair rewards and maximizing the utility of participants, as demonstrated by the Stackelberg game model.

3.5 Organizational solutions

3.5.1 Personal Data Protection Certification

As previously specified, multiple standards and legal frameworks directly affect the development and deployment of 5G vehicular networks. This multitude of reference sources and the great number of legal requirements involved generate obstacles to the interoperability and massification of V2X communications, as various jurisdictional requirements may present technical and organizational obstacles to the entry into the market of foreign solutions.

Certification has been a historical solution to enable the globalization and interoperability of technologies. By ensuring conformity criteria and incorporating these into the business practices, players in the market can ensure their products and services will be easily adopted regardless of the final location of the deployment. Personal data protection regulations, however, presents a complication to this situation, as they include both technical and organizational requirements and even incorporates security requirements and best practices that have traditionally been outside of the scope of most national legal frameworks.

As defined before, both the European approach to Personal Data Protection, as embodied in the GDPR, and the Chinese approach to privacy regulation present many such challenges to the deployment of innovative technologies in a globalized environment. From data localization requirements to limitations of trans-border data flows, the identification of a path forwards for the harmonization of both legal regimes will be key to the massification of V2X and future 5G networks as envisioned in the 5G-DRIVE project.

A potential solution to this situation can, however, be found in voluntary GDPR-specific certification schemes, which have been developed and approved in accordance to Art. 42 and 43 of the GDPR to "*demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries* (…)"(GDPR, 2016).

Europrivacy is a certification scheme developed through the Horizon 2020 European research programme with financial support from the European Commission and Switzerland. Europrivacy was developed through a sequence of European research projects, including: EAR-IT (2012-2014 on privacy risk assessment methodology), Privacy Flag (2015-2018 on certification scheme design), and ANASTACIA (2017-2019 on authenticated certificates). It was also extended and used in the context of Synchronicity, the European Large-Scale Pilot on Internet of Things for Smart Cities, to assess the compliance of smart city deployments with the GDPR.

It was co-created by several European research partners committed to promote personal data protection and to support the implementation of the GDPR. Europrivacy is managed by the European Centre for Certification and Privacy (ECCP) in Luxembourg under the guidance of an international board of experts in data protection. ECCP has been granted the status of research centre by the authorities of Luxembourg and will keep a continuous and close cooperation with the European research programme to maintain a high level of reliability of its certification scheme by leveraging on the European research community and a network of seasoned experts in data protection from all over Europe and beyond.

Europrivacy has been designed to directly encompass the whole range of requirements found in the GDPR and can easily be extended to include complementary national and domain-specific obligations, which makes it particularly relevant in the context of 5G-DRIVE. It has been designed to be comprehensive and capable of assessing a large scope of data processing activities by complementing its core list of checks and controls with complementary ones according to the Target of Evaluation. While its focus is on data processing activities (following the required approach by EDPB), its dual compliance with ISO/IEC 17065 and 17021-1 (where applicable) enables Europrivacy to assess data processing in the context of services, products, and information management systems.

Europrivacy has closely followed the EDPB recommendations regarding certification criteria generation: "*the basis for certification criteria must be derived from the GDPR principles and rules and help to provide assurance that they are fulfilled. The development of certification criteria should focus on verifiability, significance, and suitability of certification criteria to demonstrate compliance with the Regulation. The certification criteria should be formulated in such a way that they are clear and comprehensible and that they allow practical application*"[16].

Europrivacy has been designed to deliver homogeneous, consistent, and reliable certifications applicable to diverse categories of data processing activities. Beyond the core GDPR requirements, Targets of Evaluation may be subject to complementary national regulations. Particular application domains and technologies may also expose the data subjects to specific risks for their rights and freedoms. Consequently, Europrivacy is structured in a sequence of complementary criteria, checks and controls, including:

- The Europrivacy GDPR Core Criteria: which gathers the common criteria for assessing compliance with the GDPR requirements. They are mandatory and applicable to all data processing.

It is complemented by three sets of complementary requirements, namely:

- Complementary Contextual Checks and Controls: to assess compliance with the domain and technology-specific requirements. It enables to address technology and domain specific risks for the data subjects.
- Technical and Organizational Measures Checks and Controls: to assess the security measures set in place to protect the processed data.
- National Data Protection Obligations: with their complementary data protection requirements.

The following figure illustrates the complementarity between the Europrivacy GDPR Core Criteria and the complementary checks and controls.

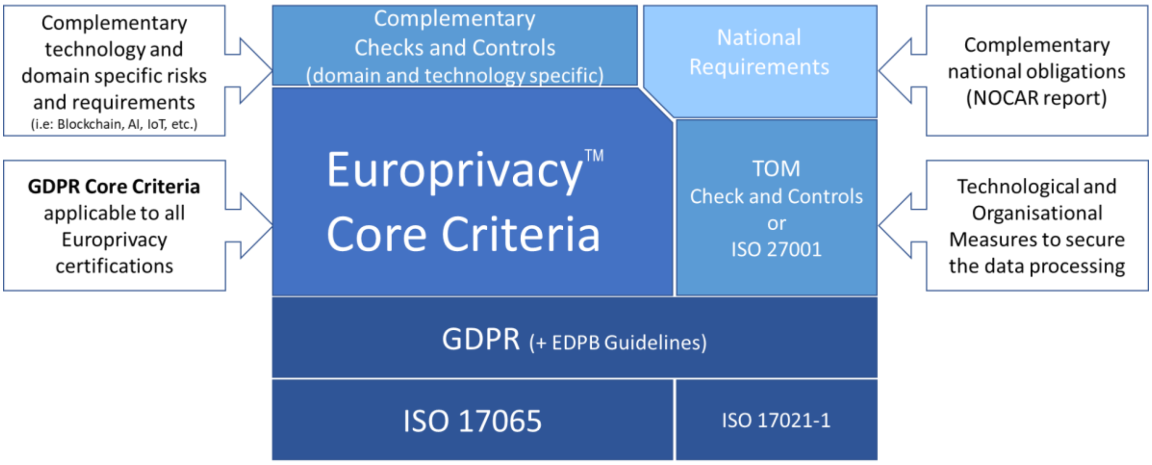

Complementary technology and domain specific risks and requirements
(i.e: Blockchain, AI, IoT, etc.)
Complementary Checks and Controls (domain and technology specific)
National Requirements
Complementary national obligations (NOCAR report)
GDPR Core Criteria applicable to all Europrivacy certifications
Europrivacy™ Core Criteria
TOM Check and Controls or ISO 27001
Technological and Organisational Measures to secure the data processing
GDPR (+ EDPB Guidelines)
ISO 17065
ISO 17021-1

Figure 54: Europrivacy Core Criteria and Complementary Requirements

The applicability of the complementary checks and controls is determined by factual and objective factors, such as the nature and location of the data processing, as illustrated in the following figure:

[16] See Page 15 - Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

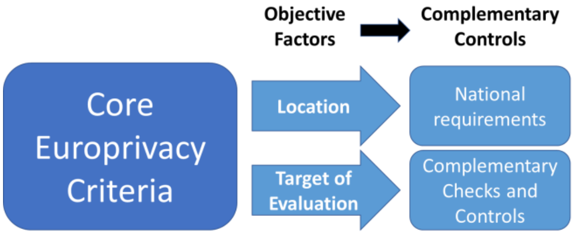


Figure 55: Complementary controls determined by objective factors

A key objective of Europrivacy criteria is to reduce the risk of subjective interpretation by the auditor. It is important to prevent the risk that two auditors certifying the same data processing may reach different conclusions.

All Europrivacy criteria were defined to meet the following principles of criteria specification:

- **Adequate** for assessing compliance with the corresponding legal requirement.
- **Auditable** by ensuring that the requirement can be effectively assessed and demonstrated.
- **Objective and factual** by focusing on verifiable facts and evidence to minimize the subjectivity in the assessment.
- **Clearly worded** to avoid any ambiguity or room for misinterpretation.
- **Homogeneously applicable** with the same relevance to diverse data processing activities and data controllers.
- **Efficient** to deliver a reliable assessment of compliance without unnecessary workload.
- **Party Neutral** by ensuring it can be used by the Applicant, the Certification Body and any other third party.

To define a new criterion, a systematic process must be followed that considers both the above-mentioned principles, as well as formatting requirements, avoiding any ambiguity. Criteria are overviewed by the Europrivacy international Board of Experts and are regularly updated to consider the evolution of the jurisprudence and the publications of the EDPB. In this context, the process of proposing technology-specific criteria extensions as undertaken by 5G-DRIVE must consider not only the state of the art on the relevant technology, but also ensuring an adequate balancing of efficiency and demonstration of compliance with the highest identified data protection requirements (e.g.: whenever incorporating nationally or sectorially defined requirements, developed criteria should not decrease the level of protection defined by the GDPR, and may raise this level if appropriate vis-à-vis the aforementioned principles of criteria specification).

In summary, all Europrivacy certifications must comply with a set of Core GDPR Criteria, which encompass the core obligations of the GDPR applicable to all data processing. Additionally, the auditor must apply complementary criteria to assess the requirements associated with specific technologies or application domains that are present in the Target of Evaluation. These domains and technology specific complementary criteria can be extended to address new technologies and jurisdictions. Following continuous discussions with the ECCP, the 5G-DRIVE project was invited to specify a set of conformity assessment criteria, which has been submitted for evaluation by the Europrivacy International Board of Experts. Upon its approval as Europrivacy complementary checks and controls, they will be submitted to the Luxembourgish Data Protection Authority for review and posterior submission to the European Data Protection Board with the goal of ensuring their widespread adoption.

The resulting extension to the Certification Scheme provides several benefits to organizations involved in the development of connected vehicles worldwide, as it will provide a streamlined and interoperable avenue to demonstrate compliance with personal data protection requirements of both Europe and other jurisdictions, simplifying the process for market entry and raising the potential of adoption of new technologies by enhancing end-user trust in innovative data processing activities.

3.5.1.1 Specification methodology for PDP conformity assessment criteria for Connected Vehicles.

The process for the generation of the technology-specific extensions to the Europrivacy Certification Scheme for connected vehicles was performed in two stages:

The first stage of the process was to identify relevant documents containing specific information and legal requirements for the connected vehicle industry with the focus on data protection and data privacy (the most relevant outcomes of this assessment has been conveyed in Section 2). This first stage involved the compilation of recommendations, guidelines, reports, and legal articles published by international institutions and organizations of the European Union, such as the European Commission, European Data Protection Board, and the European Union Agency for Cybersecurity. Secondly, the assessment examined the work (recommendations, guidelines, and other publications) of national data protection supervisory authorities of all Member States of the European Union, on how to address the initial inconsistencies and legal challenges of the connected vehicle industry. Finally, the assessment also studied the findings and proposals of national associations of the automotive industry, particularly those who have submitted codes of conduct and best practices on relevant topics for their consideration and approval by national supervisory authorities.

Once this preparatory phase was concluded, an in-depth analysis was carried out to determine the obligations and specifications mentioned by the documents. This process took place in several iterations, where requirements were extracted, compiled, and synthetized to properly convey the necessary information. This process concluded with the adaptation of the draft criteria to match the Europrivacy guidelines on criteria generation with the final goal of easing their adoption by the International Board of Experts. As the draft criteria have yet to be approved by the EDPB, 5G-Drive T5.4 will continue to address any request for modifications and updates until the end of the project and will perform a final validation of the expressed criteria through bilateral calls with consortium members before the project finalization, with the end-goal of showcasing project results and easing the adoption of this solution in real-world deployments.

3.5.1.2 Proposed Criteria

The following tables will showcase the latest draft of the proposed criteria as submitted by MI to ECCP. As mentioned in the previous sections, the Europrivacy Certification Scheme follows a hybrid approach to the organization of criteria, where core criteria tightly aligned with the GDPR requirements is complemented with technology or context-specific criteria. Some of the requirements identified in sections 2 and 3 are easily subsumed by the Core GDPR criteria, however, many have diverging approaches due to their area of applicability. For this reason, two tables will be presented, one showcasing requirement that is already addressed by the GDPR core criteria, and a second one which introduces the proposed extensions to the current Certification Scheme.

Area	Requirement	Criteria Rationale	Corresponding Criteria in Europrivacy GDPR Checks and Controls (Abridged)	Europrivacy Scheme Location	Requirement Source
Connected Vehicles	Enable Personal Data Protection Safeguards by Default	Personal Data Protection safeguards should be enabled by default for all in-vehicle data processing and V2X communications.	A) The Applicant shall have policies, rules, or procedures in place requiring to adopt data protection by design and by default for its data processing. (…)	G.6.1.1. GDPR Core Criteria	GDPR Art. 25
Connected Vehicles	Identification of data categories	Categories of processed data should be identified by the processing entity and classified based on their source and/or sensitivity.	A) The Applicant or an expert with adequate expertise shall have analyzed the categories of data processed in the Target of Evaluation in order to check and identify if it contains any Special categories of data such as: - data that reveal racial or ethnic origin; - data that reveal political opinions, religious or philosophical beliefs, or trade union membership; - genetic or biometric data for the purpose of uniquely identifying a natural person; - data on health, sex life and sexual orientation.	G.2.1.1 GDPR Core Criteria	GDPR Art. 9
Connected Vehicles	Data management / Data subject right compliance	V2X enabled vehicles, entities, vehicle manufacturers and C-ITS service providers should enable the management of personal data, data management preferences and the submission of requests to the DPO by the user/data subject.	A) The Applicant shall have a procedure or a mechanism in place to: a.1) receive and record all the requests of the data subjects; (…) AND B) The Applicant shall keep records of:	G.3.1.3. GDPR Core Criteria	Art. 12 CSL 4 CPISS GDPR Art. 12

Area	Requirement	Criteria Rationale	Corresponding Criteria in Europrivacy GDPR Checks and Controls (Abridged)	Europrivacy Scheme Location	Requirement Source
			b.1) the data subject requests with the date of reception; b.2) (AND) the communications with data subjects with their dates; b.3) (AND) the follow-up actions with their dates. b.4) (AND) if applicable, the reasons for not complying with the received request		
Connected Vehicles	Data Retention Compliance	V2X enabled vehicles, vehicle manufacturers and C-ITS service providers should implement clearly defined data retention policies for the diverse data categories handled	A) The Applicant shall have written security rules and/or policies to protect and secure the data processing that covers at least: (…) a.5) (AND) the data storage and retention period policy;	G.6.2.1. GDPR Core Criteria	6.1 CPISS GDPR Art. 32
Connected Vehicles	Data breach information	V2X enabled vehicles, entities, vehicle manufacturers and C-ITS service providers should maintain records of data breaches and comply with national regulatory requirements on data breach information to data subjects, vulnerabilities should be communicated as transparently as possible.	A) The Applicant shall have rules, a procedure or a mechanism in place to: a.1) record data breaches and follow-up actions with the date and time; (…) a.3) (AND) assess if the data breach is likely to result in a risk to the rights and freedoms of natural persons; (…) a.5) (AND) if the risk is likely to result in a risk to the rights and freedoms of natural persons, inform the data subject without undue delay (except if a GDPR Art. 34.2 exception applies).	G.7.1.2. GDPR Core Criteria	9 CPISS Art. 21(3), Art. 25, and Chapter V CSL GDPR Art. 33 ENISA Good practices for IoT and Smart Infrastructures – Section 14 & 30
Connected Vehicles	Update and review of privacy measures	V2X enabled vehicles, entities, vehicle manufacturers and C-ITS service providers shall carry out periodic	A) The Applicant shall have rules, a policy or a procedure in place to regularly test, assess and evaluate the effectiveness of the Technical and	G.6.2.3. GDPR Core Criteria	Art. 35 CSL 10.5 CPISS GDPR Art. 32

Area	Requirement	Criteria Rationale	Corresponding Criteria in Europrivacy GDPR Checks and Controls (Abridged)	Europrivacy Scheme Location	Requirement Source
		updates of privacy measures and policies	Organisational Measures at least on a yearly basis. AND B) The Applicant shall document its tests and assessments of the Technical and Organizational Measures. AND C) The Applicant shall document the identified vulnerabilities and actions taken to address these vulnerabilities. AND D) The Applicant's development lifecycle shall be planned to ensure that security and privacy are taken into account no later than the design phase.		ENISA Good practices for IoT and Smart Infrastructures – Section 20 & 43

Table 24: Overview of requirements subsumed by EP Core Criteria

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
Connected Vehicles	Data processing information or documentation	The most important information on data processing should always be made available by the manufacturer in an easy to understand form in the vehicle documentation.	A) The driver shall have access to the following information on the data processing of the Target of Evaluation: a.1) the scope and nature of the personal data processing; a.2) (AND) the purpose of its personal data processing; a.3) (AND) how to control and deactivate the personal data processing;	G.5.4.1 GDPR Core Criteria C.14.1.1	GDPR Art. 12, 13 CSL Art. 37 CPISS Art. 5.6, 6, 7 ENISA Good practices for IoT and Smart

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
			a.4) (AND) how to access and delete the stored personal data; a.5) (AND) how to contact the Data Protection Officer (DPO) of the Data Controller.		Infrastructures - Section 40
Connected Vehicles	Vehicle usage data communication	Vehicle usage data provides information on the data subject's driving style or distance covered. The consent can be obtained by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle.	IF usage data are communicated or remotely collected from the vehicle THEN: A) There shall be a mechanism or a procedure in place to ensure that prior informed consent of the owner of the vehicle is collected before the transmission of such usage data.	C.14.1.2	GDPR Art. 7 CPISS Art. 5.6
Connected Vehicles	Regular processing of geolocation data	Collection of geolocation data of a vehicle should be considered as personal data due to the fact that a vehicle location is naturally associated to the location of its driver. As a consequence, it should be highly protected as it reveals the life habits of data subjects, their place of work and residence, their centre of interest, and possibly sensitive information.	IF geolocation data are communicated or remotely collected from the vehicle THEN: A) The DPO or a qualified expert shall have assessed and validated that: a.1) the granularity of retrieved geolocation data is not more detailed than necessary to achieve the purpose of the processing; a.2) (AND) the retention period of the geolocation data is no longer than necessary to achieve the purpose of the processing. AND B) There shall be a mechanism or process in place: b.1) to ensure that the purpose of geolocation data processing is communicated to the driver; b.2) (AND) to enable the driver to deactivate the processing of geolocation data. AND C) The user interface of the vehicle shall display an	C.14.1.3	GDPR Art. 12, 13, 25 CPISS Art. 5.5, 6.3, 7.1, 7.3, 8.2, 8.4, 10.5

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
			icon to inform the data subject when geolocation data are processed.		
Connected Vehicles	Special processing of geolocation data in case of theft	The anti-theft service should not continuously collect geolocation data, but only when the data subject activates the service.	IF a mechanism is in place to enable the location of a vehicle in case of theft THEN: A) The activation and deactivation of remote geolocation of the vehicle in case theft shall be controlled by the owner of the vehicle (or by a qualified national authority).	C.14.1.4	GDPR Art. 7, 25 CPISS Art. 5.5, 5.6, 6.3, 7.1, 7.3, 8.2, 8.4, 10.5
Connected Vehicles	Tracking via in-vehicle WiFi technology	Vehicle manufacturers, due to the proliferation of Internet connection interfaces, have the possibility to offer models that include a built-in cellular data connection and are capable of creating Wi-Fi networks, which poses greater risks to the privacy of individuals. Through the vehicles, data subjects become continuous broadcasters and can be identified and tracked. In order to prevent tracking, opt out options should be put in place in the vehicle by the manufacturers	IF the vehicle contains Wi-Fi connectivity THEN: A) The driver shall have the possibility: a.1) to prevent the WiFi system of the vehicle from connecting to external access points; a.2) (AND) to deactivate the collection and storage of IP and MAC addresses of passengers.	C.14.1.5	GDPR Art. 25 CPISS Art. 7.7
Connected Vehicles	In-car applications and processing	Ensuring that personal data is processed internally in the vehicle guarantees the data subjects sole and full control of their data, while presenting lower privacy risks through prohibiting any data processing by stakeholders without the data subject knowledge.	IF the Applicant uses an in-car application platform THEN: A) There should be a mechanism in place: a.1) to inform the drivers on the personal data processed by the in-car applications; a.2) (AND) to enable the drivers to activate and deactivate the processing of personal data by the in-car applications.	C.14.1.6	GDPR Art. 7, 12, 15, 17 CPISS Art. 7.2

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
			AND B) Personal data collected by the in-car applications shall not be transmitted to any third parties, except if a specific informed consent has been given by the driver. AND C) There shall be a mechanism in place enabling the owner of the car: c.1) to have access to the personal data generated by the in-car applications; c.2) (AND) to delete the personal data collected by the vehicle before the vehicle is put up to sale.		
Connected Vehicles	Behavioural monitoring	The collection and processing of behavioural information constitutes an important source of risks for data subjects. The Applicant has the responsibility to ensure the security of data collected (i.e. through telematics box) in order to avoid the data being misused based on the creation of the driver's movement profile.	IF behavioural data are collected from the vehicle (i.e. through a telematics box), THEN: A) The driver shall be specifically informed about: a.1) the presence of behavioural monitoring; a.2) (AND) the purpose and scope of behavioural monitoring. AND B) The raw data of the driving behaviour shall be processed or pre-processed locally (in the vehicle or on the driver's personal device) in order to minimize data exposure.	C.14.1.7	GDPR Art. 25 Art. 31 CSL CPISS Art. 5.5, 6.3, 7.1, 7.3, 8.2, 8.4, 10.5
Connected Vehicles	Utilization requirements of eCall system	The eCall system enables drivers in Europe to automatically call the local emergency services in case of an accident. User manuals and manufacturers shall provide clear and complete information on data processing done using the eCall system.	IF an eCall system is included in the Target of Evaluation, THEN: A) The Applicant shall ensure that data subjects are provided with information on: a.1) the scope and purpose of data processing by the eCall; a.2) (AND) the retention period of data stored by	C.14.1.8	GDPR Art. 12, 13 CPISS Art. 5.5, 6.1

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
			the eCall system; a.3) (AND) the fact that the vehicle is not under constant surveillance; a.4) (AND) the fact that the eCall system is activated by default; a.5) (AND) the competent contact to submit a request and exercise data subject rights.		
Connected Vehicles	Securing vehicle's communications	The Applicant has an obligation to take measures to guarantee data confidentiality within the vehicle as well as to data transmitted away from the vehicle, while avoiding disclosure to unauthorized third parties. Consequently, data confidentiality and security should apply to data processed and collected within the vehicle and data transmitted away from the vehicle. Security measures for vehicle's communication system should be adapted to the risks posed by the processing and should be regularly reviewed and updated.	A) The communication system of the vehicle shall: a.1) encrypt communication channels; a.2) (AND) use authentication mechanism of the devices taking part in vehicle communication; a.3) (AND) use authentication mechanism of servers authorized to perform firmware/software patches and updates; a.4) (AND) where applicable, use of frequencies allocated to vehicles communication.	C.14.1.9 T.1.1.8	CSL 21 GDPR Art. 25, 32 CPISS Art. 6.3, 10.3 ePrivacy Art. 5
Connected Vehicles	Other security measures	The service provider should be able to put in place measures that guarantee the security and confidentiality of data processing and should take all necessary precautions to prevent control from being taken by an unauthorised person. The measures put in place should be adapted to the	A) The car shall include the following security measures: a.1) it shall partition the vehicle's vital functions from those relying on telecommunication capacities; a.2) (AND) it shall require user authentication to access the stored personal data; a.3) (AND) it shall include a system or solution to	C.14.1.10	CSL 21 GDPR Art. 25, 32 CPISS Art. 6.3, 10.3 ePrivacy Art. 5

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
		level of data sensitivity.	detect and alert in case of intrusions in the data management system of the vehicle. a.4) (AND) it shall enable remote patching of firmware and software vulnerabilities during the lifespan of the vehicle; a.5) (AND) it shall store a log history of access to the vehicle's information system.		ENISA Good practices for IoT and Smart infrastructure Section 16
Connected Vehicles	Biometric data restrictions	The Applicant should ensure that biometric data is protected against unauthorized access. I particular, biometric data should not be stored in raw format, but should use instead cryptographic functions (i.e. hash function) or other similar solutions.	IF biometric data is used in connected vehicles THEN: A) The data subject shall be able to use a non-biometric alternative. AND B) The biometric data: b.1) shall not be transmitted to a remote server; b.2) (AND) shall not be stored in clear format. AND C) The risk related to the use of biometric data in the processing shall have been assessed in the context of a Data Protection Impact Assessment (DPIA)	C.14.1.11	GDPR Art. 9 CPISS Art. 5.5, 6.3, 7.1, 7.3, 8.2, 8.4, 10.5
Connected Vehicles	Data processing revealing criminal offenses or other infractions	Personal data which relates to potential criminal offences should be processed locally where the data subject has full control over the processing.	A) The Data Processing Impact Assessment shall have evaluated the risk for the data subjects that the data processing of the vehicle communicates criminal offenses or other infractions.	G.8 GDPR Core Criteria C.14.1.12	GDPR Art. 10 CPISS Art. 5.5, 6.3, 7.1, 7.3, 8.2, 8.4, 10.5
Connected Vehicles	Protection of communications and traffic data	Traffic and communication data should only be processed by the V2X entity/network provider. Procedures	IF V2X communications are implemented, THEN: A) The Applicant shall have rules, policies, contractual clauses, guidelines, or mechanisms in	G.6.2.10. GDPR Core Criteria	CSL Art. 31 ePrivacy Directive Art.

Area	Requirement	Criteria Rationale	Proposed Criteria	Europrivacy Scheme Location	Requirement Source
		such as anonymization and pseudonymization should be implemented to ensure non-identifiability, minimum disclosure, unlinkability, and forward and backward privacy.	place to ensure the processing of traffic data is only performed by authorized entities or service providers. AND B) The applicant shall implement technical measures to: b.1) prevent the identification or re-identification of vehicles or users; b.2) (AND) minimize information disclosure to the bare minimum for system operation; b.3) (AND) prevent linking of the diverse pseudonyms assigned to a vehicle; b.4) (AND) ensure that credential revocation does not affect the unlinkability of previously signed messages.	Contextual Checks and Controls	9 GDPR Art. 32 CPISS Art. 6.1(b) ENISA Good practices for IoT and Smart Infrastructures Tool - Section 32 5GAA Privacy by Design Aspects of V2X

Table 25: Overview of proposed criteria extension for connected vehicles

4 Conclusions

This deliverable presented the research performed on security and personal data protection by WP5 partners. Following the introductory considerations and the methodology specified in Section 1, Section 2 performed an in-depth analysis of the general context surrounding security and personal data protection in 5G Vehicular Networks, including an in-depth legal analysis of the relevant legal frameworks (UN, EU and China), and introducing some of the salient standards and recommendations that relate to the subject.

Based on this, Section 3.1 identified a main set of requirements for personal data protection compliance in connected vehicles and the fundamental requirements for V2X Security. Section 3.2 connects this analysis with the work and trials undertaken by 5G-DRIVE through a high-level data protection assessment. These elements serve to identify key issues (section 3.3) that have been considered during the proposal of potential solutions.

Two main sets of potential solutions have been proposed by 5G-DRIVE T5.4, and are presented as part of sections 3.4 and 3.5. Section 3.4 presented technical solutions whic tackle not only location privacy protection and misbehavior detection systems but also trust and data protection for 5G vehicular networks. In addition, most of the proposed solutions consider the context and the current situation of vehicles to change the security parameters thanks to the SDN paradigm. The rest of them leverage blockchain to enable trusted interaction between connected vehicles.

The first two solutions (subsections 3.4.1 and 3.4.2) address location privacy issues in 5G vehicular networks. Subsection 3.4.1 presented a strategy that provides a collaborative changing of pseudonyms to maximize location privacy protection. This strategy leverages the SDN control plane to tune security parameters. Subsection 3.4.2 presented a solution that suggests changing pseudonyms in specific zones called VLPZs. Specifically, this solution proposes to install a genetic algorithm at the level of the SDN controller to dynamically manage the placement of VLPZs over gas stations by considering the mobility of vehicles, the positions, and capacities of gas stations. As a complementary work of the two previous solutions, subsection 3.4.5 presented an SDN-based privacy protection framework for 5G vehicular networks. This solution proposes a global picture of the internal architecture of the SDN controller for a context-aware use of pseudonym-changing strategies.

Subsection 3.4.3 presented a situation-centric and dynamic misbehavior detection system for 5G vehicular networks. This solution leverages the SDN control plane to dynamically deploy watchdogs equipped with trust models to detect internal attacks accurately. Subsection 3.4.4 presented a solution that proposes adding a blockchain layer to provide trusted interaction between vehicles in pseudonym-changing processes (PCPs). More specifically, this solution leverages a consortium blockchain-enabled fog layer and smart contracts to incentivize non-cooperative vehicles to change their pseudonyms within PCPs. In addition, this solution exploits a lightweight consensus protocol to provide a scalable blockchain system.

Subsection 3.4.6 presented a solution that combines SDN and blockchain for secure data trading in 5G vehicular networks. Specifically, this solution designs data-trading smart contracts between data providers (vehicles) and data requesters (vehicles) and proposes a consensus mechanism to deploy them on the blockchain system. In addition, this solution leverages the SDN control plan to optimize the placement of fog stations.

Finally, Section 3.5 it introduces certification as a potential organizational solution to the current regulatory divides across the relevant jurisdictions and personal data protection frameworks. Personal Data Protection certifications may serve as a key enabler towards ensuring trustable cross-border data transfers, easing entry into the EU Digital Single Market market for non-EU solution providers. To this end it proposes a technology-specific criteria extension for the Europrivacy GDPR Certification Scheme which have been presented for approval by the European Data Protection

Board for their eventual adoption as part of an European Data Protection Seal as defined in GDPR Art. 42.

This deliverable may then conclude that the adoption of the proposed technical and organizational solutions by the industry could help to enhance trust and demonstrate compliance across the various stakeholders involved in the connected vehicle ecosystem.

5 References

5G cross border corridors | Shaping Europe's digital future. (2021, September 3). https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors

5GAA. (2020). *Privacy by Design Aspects of C-V2X*. 5GAA; 29/10/2020. https://5gaa.org/wp-content/uploads/2020/11/5GAA_White-Paper_Privacy_by_Design_V2X.pdf

About: C-Roads. (n.d.). Retrieved May 13, 2021, from https://www.c-roads.eu/platform/about/about.html

About IEEE. (n.d.). Retrieved May 12, 2021, from https://www.ieee.org/about/index.html

Advertising Law of the People's Republic of China. (1994, October). http://english.mofcom.gov.cn/aarticle/lawsdata/chineselaw/200211/20021100053452.html

Ahmed, S. A. M., Syed Ariffin, S. H., & Fisal, N. (2013). Overview of Wireless Access in Vehicular Environment (WAVE) Protocols and Standards. *Indian Journal of Science and Technology*, *7*. https://doi.org/10.17485/ijst/2013/v6i7.18

Alioua, A., Senouci, S.-M., Moussaoui, S., Sedjelmaci, H., & Boualouache, A. (2017). Software-Defined heterogeneous vehicular networks: Taxonomy and architecture. *2017 Global Information Infrastructure and Networking Symposium (GIIS)*, 50–55. https://doi.org/10.1109/GIIS.2017.8169805

Alnasser, A., Sun, H., & Jiang, J. (2019). Cyber Security Challenges and Solutions for V2X Communications: A Survey. *Comput. Networks*, *151*, 52–67. https://doi.org/10.1016/j.comnet.2018.12.018

Andrea Jellinek. (2019). *Statement 3/2019 on an ePrivacy Regulation*. European Data Protection Board.

Automated driving in focus at 2021 Symposium on the Future Networked Car. (2021, May 3). https://www.itu.int:443/en/myitu/News/2021/03/05/13/53/Automated-driving-in-focus-at-2021-Symposium-on-the-Future-Networked-Car

Booz Allen Hamilton. (2019). *Driving away with your data. Privacy and connected vehicles.* [White Paper]. https://iapp.org/media/pdf/resource_center/Privacy_and_Connected_Vehicles.pdf

Boualouache, A., Senouci, S.-M., & Moussaoui, S. (2020). PRIVANET: An Efficient Pseudonym Changing and Management Framework for Vehicular Ad-Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, *21*(8), 3209–3218. https://doi.org/10.1109/TITS.2019.2924856

Boualouache, Abdelwahab, & Moussaoui, S. (2016). Urban pseudonym changing strategy for location privacy in VANETs. *International Journal of Ad Hoc and Ubiquitous Computing*, *24*(1/2), 49–64. https://doi.org/10.1504/IJAHUC.2017.080914

Boualouache, Abdelwahab, & Moussaoui, S. (2017). TAPCS: Traffic-aware pseudonym changing strategy for VANETs. *Peer-to-Peer Networking and Applications*, *10*(4), 1008–1020. https://doi.org/10.1007/s12083-016-0461-4

Boualouache, Abdelwahab, Senouci, S.-M., & Moussaoui, S. (2017). A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks. *ArXiv:1704.00679 [Cs]*. http://arxiv.org/abs/1704.00679

Commission endorses EU toolbox to secure 5G networks. (2020, January 29). [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

Connected and automated mobility | Shaping Europe's digital future. (2021, April 30). https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility

Connected and automated mobility: Three 5G Corridor trial projects to be launched at ICT 2018 event | Shaping Europe's digital future. (2018, December). https://digital-strategy.ec.europa.eu/en/news/connected-and-automated-mobility-three-5g-corridor-trial-projects-be-launched-ict-2018-event

Creemers, R., Shi, M., & Webster, G. (2020, October 21). *China's Draft "Personal Information Protection Law" (Full Translation)*. New America. http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/

Creemers, R., Triolo, P., & Webster, G. (2018, June 29). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Cybersecurity of 5G networks—EU Toolbox of risk mitigating measures | Shaping Europe's digital future. (2020, January). https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Eclipse SUMO - Simulation of Urban MObility. (n.d.). Eclipse SUMO - Simulation of Urban MObility. Retrieved May 19, 2021, from https://www.eclipse.org/sumo/

EDPB. (2020). *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

ELKI Team. (n.d.). *Same-Size K-Means*. Retrieved May 19, 2021, from https://elki-project.github.io/tutorial/same-size_k_means

ETSI. (2013a). *Automotive Intelligent Transport | Intelligent Transport Systems (ITS)*. ETSI. https://www.etsi.org/technologies/automotive-intelligent-transport

ETSI. (2013b). *ETSI TS 101 539-1 V1.1.1 (2013-08) - Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification*. ITeh Standards Store. https://standards.iteh.ai/catalog/standards/etsi/8d6a7368-2909-4f70-b7fe-aea47803ad30/etsi-ts-101-539-1-v1-1-1-2013-08

ETSI. (2017). *ETSI TR 102 893 V1.2.1*. https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

ETSI - Standards, mission, vision, direct member participation. (n.d.). ETSI. Retrieved May 12, 2021, from https://www.etsi.org/about

European Commission. (2016, January 26). *Commission launches GEAR 2030 to boost competitiveness and growth in the automotive sector* [Text]. Internal Market, Industry, Entrepreneurship and SMEs - European Commission. https://ec.europa.eu/growth/content/commission-launches-gear-2030-boost-competitiveness-and-growth-automotive-sector-0_en

Proposal for Regulation on Privacy and Electronic Communication, Pub. L. No. 2017/003 (COD) (2017).

European Commission. (2019). *Commission Staff Working Document—Ex post evaluation of the Intelligent Transport System Directive 2010/40/EU* (SWD(2019) 369 final; p. 115). European Commission.

European Commission. (2020, December 16). *New EU Cybersecurity Strategy* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Council. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

European Data Protection Board. (2019). *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*. European Data Protection Board. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en

European Data Protection Board. (2021, September 3). *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en

European Parliament. (2002, December 6). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic* *communications)*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

General Data Protection Regulation, Pub. L. No. 2016/679 (2016).

European Parliament. (2016). *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

European Parliament. (2018, December 17). *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance*. https://eur-lex.europa.eu/eli/dir/2018/1972/oj

European Parliament. (2019, April 17). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016). http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

European Telecommunications Standards Institute. (2018). *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management* (Technical Specification ETSI TS 102 940 V1.3.1 (2018-04); p. 42).

European Telecommunications Standards Institute. (2019). *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management* (ETSI TS 102 941 V1.3.1 (2019-02); p. 73). ETSI.

European Union Agency for Cybersecurity. (2019, November 25). *ENISA good practices for security of Smart Cars* [Report/Study]. https://www.enisa.europa.eu/publications/smart-cars

European Union Agency for Cybersecurity. (2021a, May 5). *Recommendations for the security of CAM* [Report/Study]. https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

European Union Agency for Cybersecurity. (2021b, November 2). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving* [Press Release]. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving

Freudiger, J., Manshaei, M. H., Hubaux, J.-P., & Parkes, D. (2009). On Non-cooperative Location Privacy: A Game-theoretic Analysis. *Proceedings of the ACM Conference on Computer and Communications Security*. https://doi.org/10.1145/1653662.1653702

Garey, M. R., & Johnson, D. S. (1990). *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co.

How automated driving can pave the way for safe mobility. (2021, March 30). https://www.itu.int:443/en/myitu/News/2021/03/30/07/43/Automated-driving-safe-mobility-connected-car

Huang, X., Yu, R., Pan, M., & Shu, L. (2018). Secure Roadside Unit Hotspot Against Eavesdropping Based Traffic Analysis in Edge Computing Based Internet of Vehicles. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2868002

Huq, N., Gibson, C., Kropotov, V., & Vosseler, R. (2021). *Cybersecurity for Connected Cars. Exploring risks in 5G, cloud, and other connected technologies*. https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf

IBM. (2019, April 22). *Helping to secure privacy for data generated by connected cars*. IBM. https://www.ibm.com/thought-leadership/institute-business-value/report/car-privacy

IEEE. (n.d.). *Home | ICCVE 2019*. Retrieved May 14, 2021, from http://iccve2019.com/

IEEE 1609.2.1-2020—IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Certificate Management Interfaces for End Entities. (n.d.). Retrieved May 12, 2021, from https://standards.ieee.org/standard/1609_2_1-2020.html

IEEE 1609.3-2020—IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking. (n.d.). Retrieved May 12, 2021, from https://standards.ieee.org/standard/1609_3-2020.html

IEEE 1609.4-2016—IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation. (n.d.). Retrieved May 12, 2021, from https://standards.ieee.org/standard/1609_4-2016.html

IEEE 1609.12-2019—IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Identifiers. (n.d.). Retrieved May 12, 2021, from https://standards.ieee.org/standard/1609_12-2019.html

IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. (2019). *IEEE Std 1609.0-2019 (Revision of IEEE Std 1609.0-2013)*, 1–106. https://doi.org/10.1109/IEEESTD.2019.8686445

IEEE Innovation at Work. (2020, May 14). How Can Autonomous Vehicles Be Protected Against Cyber Security Threats? *IEEE Innovation at Work*. https://innovationatwork.ieee.org/how-can-autonomous-vehicles-be-protected-against-cyber-security-threats/

IEEE Spectrum. (2020, October 21). *Learn How to Protect Autonomous Vehicles Against Hackers—IEEE Spectrum*. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/the-institute/ieee-products-services/learn-how-to-protect-autonomous-vehicles-against-hackers

IEEE Standard for Wireless Access in Vehicular Environments (WAVE)– Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS). (2011). *IEEE Std 1609.11-2010*, 1–62. https://doi.org/10.1109/IEEESTD.2011.5692959

IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. (2016). *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, 1–240. https://doi.org/10.1109/IEEESTD.2016.7426684

International Organization for Standardization. (2008). *ISO/TS 25237:2008 Health informatics—Pseudonymization*. https://www.iso.org/standard/42807.html

International Organization for Standardization. (2013a). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/standard/54534.html

International Organization for Standardization. (2013b). *ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls*. https://www.iso.org/standard/54533.html

International Standardization Organization. (n.d.-a). *ISO/CD 24089*. ISO. Retrieved May 14, 2021, from https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/77/77796.html

International Standardization Organization. (n.d.-b). *ISO/SAE FDIS 21434*. ISO. Retrieved May 14, 2021, from https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/09/70918.html

International Standardization Organization. (2009). *ISO/TR 12859:2009 Intelligent transport systems—System architecture—Privacy aspects in ITS standards systems*.

International Standardization Organization. (2010). *ISO 24100:2010 Intelligent transport systems—Basic principles for personal data protection in probe vehicle information services*.

International Standardization Organization. (2015a). *ISO/IEC 29190:2015(en), Information technology—Security techniques—Privacy capability assessment model*. https://www.iso.org/obp/ui#iso:std:iso-iec:29190:ed-1:v1:en

International Standardization Organization. (2015b). *ISO/TR 17427-7:2015 Intelligent transport systems—Cooperative ITS - Part 7: Privacy aspects*.

International Standardization Organization. (2018). *ISO 16461:2018 Intelligent transport systems—Criteria for privacy and integrity protection in probe vehicle information systems*.

International Standardization Organization. (2019). *ISO/IEC 27701:2019 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*.

IONOS. (2020, May 2). *ePrivacy Regulation: About the EU's privacy policy*. IONOS Digitalguide. https://www.ionos.com/digitalguide/websites/digital-law/eprivacy-regulation-about-the-eus-privacy-policy/

ISO/IEC 27000:2018(en), Information technology—Security techniques—Information security management systems—Overview and vocabulary. (n.d.). Retrieved May 12, 2021, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ISO/IEC 27005:2018(en), Information technology—Security techniques—Information security risk management. (2018). https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27005:ed-3:v1:en

Jemaa, I. B., Kaiser, A., & Lonc, B. (2017). Study of the impact of pseudonym change mechanisms on vehicular safety. *2017 IEEE Vehicular Networking Conference (VNC)*, 259–262. https://doi.org/10.1109/VNC.2017.8275632

Jiang, M. (2019). *Cybersecurity Policies in China* (SSRN Scholarly Paper ID 3523325). Social Science Research Network. https://papers.ssrn.com/abstract=3523325

Lee, J.-A. (2018). Hacking into China's Cybersecurity Law. *Wake Forest Law Review*, *53*(1), 48.

Lee, S.-W., Kwon, H.-C., & Na, J.-C. (2017). Standardization Issues on Secure Vehicular Communication. *International Journal of Communications*, *02*. https://www.iaras.org/iaras/journals/caijoc/standardization-issues-on-secure-vehicular-communication

Lefevre, S., Petit, J., Bajcsy, R., Laugier, C., & Kargl, F. (2013). Impact of V2X privacy strategies on Intersection Collision Avoidance systems. *Fifth IEEE Vehicular Networking Conference, VNC 2013*, 71–78. https://doi.org/10.1109/VNC.2013.6737592

Lu, R., Lin, X., Luan, T. H., Liang, X., & Shen, X. (2012). Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *Vehicular Technology, IEEE Transactions On*, *61*, 86–96. https://doi.org/10.1109/TVT.2011.2162864

Luo, Y., Yu, Z., & Shepherd, N. (2019a, May 28). *China Releases Draft Measures for Data Security Management*. Inside Privacy. https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administration-of-data-security/

Luo, Y., Yu, Z., & Shepherd, N. (2019b, June 13). *China Seeks Public Comments on Draft Measures related to the Cross-border Transfer of Personal Information*. Inside Privacy. https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-on-security-assessment-for-the-cross-border-transfer-of-personal-information/

Luo, Yan, & Zhijing, Y. (2020, April 27). *China Issues New Measures on Cybersecurity Review of Network Products and Services*. Inside Privacy. https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/

Marojevic, V. (2018). C-V2X Security Requirements and Procedures: Survey and Research Directions. *ArXiv:1807.09338 [Cs, Eess]*. http://arxiv.org/abs/1807.09338

New recommendations for a safe and ethical transition towards driverless mobility. (n.d.). [Text]. European Commission - European Commission. Retrieved May 13, 2021, from https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en

People's Republic of China General Administration of Quality Supervision, Inspection and Quarantine, China National Standardization Administration. (2017, December 29). *Information security technology—Personal information security specification GB/T 35273-2017*. https://www.chinesestandard.net/PDF/English.aspx/GBT35273-2017

Petit, J., Broekhuis, D., Feiri, M., & Kargl, F. (2015). *Connected Vehicles: Surveillance Threat and Mitigation*. /paper/Connected-Vehicles-%3A-Surveillance-Threat-and-Petit-Broekhuis/396f2c169d213840c6a89e9124fd9d8bcca2942b

Privacy International. (2019). *Welcome to 5G: Privacy and security in a hyperconnected world (or not?)*. http://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not

Publications Office of the European Union. (2019, May 6). *Data protection certification mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679 : final report.* [Website]. Publications Office of the European Union. http://op.europa.eu/en/publication-detail/-/publication/5509b099-707a-11e9-9f05-01aa75ed71a1/language-en

Rafaelof, E., Creemers, R., Sacks, S., Tai, K., Webster, G., & Neville, K. (2020, February 6). *Translation: China's "Data Security Law (Draft)."* New America. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

SAE International. (2016). *J2945/1: On-Board System Requirements for V2V Safety Communications*. https://www.sae.org/standards/content/j2945/1_201603/

Schmittner, C., & Macher, G. (2019). Automotive Cybersecurity Standards—Relation and Overview. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, & F. Bitsch (Eds.), *Computer Safety, Reliability, and Security* (Vol. 11699, pp. 153–165). Springer International Publishing. https://doi.org/10.1007/978-3-030-26250-1_12

Setting the standards for autonomous driving. (2021, March 19). https://www.itu.int:443/en/myitu/News/2021/03/19/03/06/Setting-the-standards-for-autonomous-driving

Sommer, C., German, R., & Dressler, F. (2011). Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/TMC.2010.133

Tsakalakis, N., Stalla-Bourdillon, S., & O'Hara, K. (2017). Identity Assurance in the UK: Technical implementation and legal implications under eIDAS. *Journal of Web Science*, *3*(1), 32–46. https://doi.org/10.1561/106.00000010

UNECE. (n.d.). *Automated driving*. Retrieved May 14, 2021, from https://unece.org/automated-driving

UNECE. (2020, June 24). *UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles | UNECE*. https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles

University of Luxembourg. (2019). *D.4.3—Report on Potential Vulnerabilities of V2X Communications*. 5G-Drive consortium. https://5g-drive.eu/download/3277/

X.1371: Security threats to connected vehicles. (2020, May 29). https://www.itu.int/rec/T-REC-X.1371-202005-I/en

X.1372: Security guidelines for vehicle-to-everything (V2X) communication. (2020, March 26). https://www.itu.int/rec/T-REC-X.1372-202003-I/en

X.1373: Secure software update capability for intelligent transportation system communication devices. (2017, March 30). https://www.itu.int/rec/T-REC-X.1373-201703-I/en

X.1374: Security requirements for external interfaces and devices with vehicle access capability. (2020, October 29). https://www.itu.int/rec/T-REC-X.1374-202010-I/en

X.1375: Guidelines for an intrusion detection system for in-vehicle networks. (2020, 20). https://www.itu.int/rec/T-REC-X.1375-202010-I/en

X.1376: Security-related misbehaviour detection mechanism using big data for connected vehicles. (2021, July 1). https://www.itu.int/rec/T-REC-X.1376-202101-I/en

Ying, B., Makrakis, D., & Hou, Z. (2015). Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks. *IEEE Transactions on Vehicular Technology*, *64*(12). https://trid.trb.org/view/1377987

Zhang, J., Huang, X., Ni, W., Wu, M., & Yu, R. (2019). VeSenChain: Leveraging Consortium Blockchain for Secure and Efficient Vehicular Crowdsensing. *2019 Chinese Control Conference (CCC)*, 6339–6344. https://doi.org/10.23919/ChiCC.2019.8865989

Zhang, L., & Hemberg, E. (2019). Investigating algorithms for finding nash equilibria in cyber security problems. *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, 1659–1667. https://doi.org/10.1145/3319619.3326851

Zhao, Y., & Wagner, I. (2019). On the Strength of Privacy Metrics for Vehicular Communication. *IEEE Transactions on Mobile Computing*, *18*(2), 390–403. https://doi.org/10.1109/TMC.2018.2830359