Validation platform for vehicle secure and highly trusted communications in the context of the cooperative ITS systems

Farah Haidar

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2020IPPAT011

Thèse de doctorat

Validation Platform for Vehicle Secure and Highly Trusted Communications in the Context of the Cooperative ITS Systems

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à Télécom ParisTech

École doctorale n°626 Institut Polytechnique de Paris (ED IP Paris)
Spécialité de doctorat: Informatique, Données, IA

Thèse présentée et soutenue à Paris, le 06/07/2020, par

FARAH HAIDAR

Composition du Jury :

Serge CHAUMETTE professeur, Université de Bordeaux	président
Madjid BOUABDALLAH professeur, université de technologie de Compiègne (UTC)	Rapporteur
Nora CUPPENS professeur, Télécom Bretagne	Rapporteur
Houda LABIOD professeur, Télécom ParisTech	Examinateur
Pascal URIEN professeur, Télécom ParisTech	Directeur de thèse
Brigitte LONC expert Cyber securité, GROUPE RENAULT	Encadrante de thèse
Arnaud KAISER Docteur, IRT SystemX	Encadrant de thèse

Acknowledgements

Perusing my Ph.D in Cybersecurity for C-ITS helped me discover the world of research, reinforce my strengths, and transform my weaknesses into strengths! A thesis is a long-way journey that can only be achieved with perseverance, huge efforts, support, and guidance.

I would like to first address all my thanks to my thesis director, Prof. Pascal URIEN, for his consistent guidance. I also express my sincere gratitude to my PhD supervisors, Dr. Brigitte LONC and Dr. Arnaud KAISER, for the fruitful discussions, valuable advices, and for sharing their knowledge and experience with me.

I had the opportunity to work in three entities (Renault, Telecom Paris, IRT SytemX) which enriched my network of friends and colleagues that I want to thank each and everyone of them. Special thanks to Alain CLAES and Farah BRAITEH from Renault, and Ines,Joseph, Nabil, Francesca from IRT SystemX, Hafeda from Atos, Marios from Yogoko and Michel from Trialog.

My heartfelt thanks to my parents, my brothers Bassem, Ali, and Abdallah; as well as, my sister, Zeinab, for their inspiration, motivation, and support throughout my life.

I greatly acknowledge and appreciate the support I had from my beloved future husband and best friend, Karim Francois, who lived all the Ph.D stages with me from stress to hard work and success. I am extremely thankful and grateful to you.

I would like to extend my gratitude to the reviewers, Prof. Madjid BOUABDALLAH and Prof. Nora CUPPENS, for accepting to evaluate my thesis. My earnest thanks are also due to Prof. Houda LABIOD and Prof. Serge CHAUMETTE for accepting to be members of the jury.

Thanks to everyone for helping me grow into the strong woman I am today!

Contents

List of Figures

Chapter 1

GLOSSAIRE

- ITS: Intelligent Transportation Systems
- C-ITS: Cooperative-Intelligent Transportation Systems
- ITS-S: Intelligent Transportation Systems-Station
- PDU: Protocol Data Unit
- ITS-ID: ITS- Identity
- PKI: Public Key Infrastructure
- SCMS: Security Credential Management System
- CA: Certificate Authority
- RCA: Root Certificate Authority
- EA: Enrollment Authority
- AA: Authorization Authority
- CRL: Certificate Revocation List
- CTL: Certificate Trust List
- ECTL: Extended Certificate Trust List
- EC: Enrollment Certificate
- AT: Authorization Authority (eg. pseudonym certificate).
- CAM: Cooperative Awareness Message
- DENM: Decentralized Environmental Notification Message.
- SPAT: Signal Phase and Timing

- MAP: Map data
- TLM : Trust List Manager
- CPOC: C-ITS Point Of Contact
- CPA: Certificate Policy Authority
- DC: Distribution center
- MA: Misbehavior Authority
- RSA: Rivest–Shamir–Adleman
- DSA: Digital Signature Algorithm
- WAVE: Wireless Access in Vehicular Environments
- GPS: Global Positioning System
- EBIOS: Expression des Besoins et Identification des Objectifs de Securite
- TVRA: Threat Vulnerability Risk Assessment
- TOE: Taget Of Evaluation
- OBE: On-Boad-Equipment
- OBU: On-Boad-Unit
- SCMS: Security Credential Management System
- ETSI: European Telecommunication Standard Institute
- IEEE: Institute of Electrical and Electronics Engineers
- UC: Use Case
- HSM: Hardware Security Module
- LA: Linkage Authority

Chapter 2

Introduction

Intelligent Transport Systems (ITS) refer to the integration of information and communication technologies with transport infrastructure to improve road safety, mobility and environmental sustainability for the benefit of all road users. Cooperative-ITS (C-ITS) applications are based on vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and Vehicle-to-Center (V2C) wireless communications using various technologies, such as short-range wireless communication, cellular wide area networks or other broadcasting network (e.g. GNSS). Based on the exchanged messages, the C-ITS applications will first provide better awareness to drivers via road hazard warnings and traffic information, and later support cooperative driving systems and more automatic systems for the Connected Autonomous Vehicles (CAV).

Despite the many potential benefits of C-ITS, the associated wireless communications raise security and privacy issues which, if not addressed, could jeopardize their deployment. As the main target of C-ITS and CAV is to highly contribute to road safety helping to avoid accidents (collision avoidance) and to enhance the support for secondary road safety functions (pre-crash for example), a good balance between security, privacy and performances of safety related applications has to be found.

For securing C-ITS communications, standardization bodies such as the European Telecommunication Standard Institute (ETSI) and the Institute of Electrical and Electronics Engineers (IEEE) use asymmetric cryptography and this requires setting up a Public Key Infrastructure (PKI) for the management of security credentials of the ITS Station (ITS-S). The use of PKI guarantees authentication and non-repudiation by using digital signature, confidentiality by using encryption methods. However, the PKI can not solve all security problems.

Another major issue to consider is the user's privacy. Any security credential management system must consider a privacy preserving scheme to protect user private information, such as user/vehicle identity, trips or behavior, according to national and international legislation. The existing solution for privacy protection is the use of pseudonym identity during the communication. One of the main challenges is to insure that the system is really operable using the pseudonym certificates solution and if this solution can really guarantee user's privacy.

2.1 Problem statement and motivation

Embedded vehicle systems are now connected and are becoming more exposed to external attacks through wireless networks and communications with Information Systems, or through mobile devices whose security is insufficient and offers limited confidence. V2X cooperative applications and autonomous vehicles require the development of powerful and robust security, privacy and trustworthiness techniques (plausibility of exchanged data, detection of misbehaving stations, privacy protection techniques). On the other hand, existing security and privacy solution proposed by ETSI or IEEE may guarantee a good level of security and privacy but the performance analysis of those solutions should also be studied especially in a real environment. The first step of the thesis is to contribute to the security, and privacy validation, and the second step is to validate the performance of existing solutions.

2.2 Contributions

This section presents the main contribution of this thesis. The work is divided into four tasks in order to achieve the final goal.

2.2.1 Use Case Study and Classification

In C-ITS domain, a use case is a specific situation in which the system could be potentially used. For example, the roadwork warning, pre-crash warning etc are considered as use cases. To understand the automotive point of view in treating some problems in C-ITS domain, it is important to precise the supported use cases.

Many projects, standards, and consortiums have proposed some use cases. However due to the very large number of existing use cases, treating each use case separately is a tedious task. By reducing the list of use cases the treatment can become faster.

Thus, the first task in this thesis is to analyze the security and functional requirements of existing use cases and propose a clear methodology to classify them based on their requirements. This classification permits selecting some representative use cases that we should work on for the rest of the thesis [3].

2.2.2 Risk Assessment of Pseudonymity Aspects

The second contribution of this thesis is to conduct a risk assessment on selected use cases. A risk assessment is a method used to identify and analyze potential threats and vulnerabilities. It is important to understand and measure the impact of involved risks and decide on the appropriate measures and controls to manage them. In this thesis, we applied the Threat Vulnerability Risk Assessment (TVRA) method on the use cases studied and classified during the first contribution (Use case study and classification). The risk assessment helped in finding new important vulnerabilities and threats that were not taken into account [4].

2.2.3 Attack Implementation

The third contribution consists of implementing critical attacks issued from the risk analysis done in the second contribution. Implementing the attacks help us to know the origin of the problem and how to solve it. The implemented attacks are: Sybil attack [5], [6], tracking attack, exhaust of the pseudonym pool of the vehicle, and Certificate Revocation List (CRL) substitution.

2.2.4 Performance Evaluation of Pseudonym Certificate Reloading

In order to protect driver's privacy, vehicles use pseudonym certificates and change them frequently in such a way that it becomes much harder to track a vehicle. As pseudonym certificates are frequently changed, vehicles need to communicate with the PKI to reload their pseudonym pool. The communication can be done on ITS-G5 or cellular communication. For the ITS-G5, it can be done using two communication profiles: profile with geo-networking and profile without geo-networking. The forth contribution of this thesis is a performance evaluation of the pseudonym certificate reload [7] [8]. Test are conducted in two setups: the first one is over ITS-G5 technology and the second one is over cellular technology. We compared also the two communication profiles cited before (with and without geo-networking).

2.2.5 Outline

This thesis is composed of six chapters. Chapter 3 review the literature in order to give a clear view on vehicular networks, communication entities, security architecture, standardization and projects communities working on C-ITS security. Chapter 4 presents the proposition of new C-ITS use cases and a classification methodology based on security, and technical requirements. Chapter 5 presents a risk analysis study on selected use cases. Chapter 6 presents the implemented attacks, with all the details that allow performing such attacks. Chapter 7 presents the performance evaluation of pseudonym reloading from the PKI. Chapter 6 presents the conclusion of this thesis.

Chapter 3

State of the art on C-ITS

Cooperative Intelligent Transportation Systems (C-ITS) is one emerging field that enables vehicles to interact directly with each other and with the surrounding road infrastructure. In road transport, C-ITS typically involves vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and/or infrastructure-to-infrastructure (I2I) communication, and communication between vehicles and pedestrians or cyclists. Those communications are also known as vehicle-to-everything (V2X). This involves a wide range of information and cooperative services. C-ITS is a category of ITS services, based on an open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations. The security of V2X communications is based on the use of a vehicular Public Key Infrastructure (PKI) that delivers digital certificates to the vehicles in order to use them in the communication. This chapter presents a general state of the art of C-ITS, more precisely, the following aspects are studied: communication entities, security and privacy, standardization activities in Europe and USA and state of art on C-ITS vulnerabilities.

3.1 Communication entities and environment characteristics

3.1.1 Communication entities

A C-ITS consists of entities presented in figure 3.1 and listed below:

- On-Board Unit (OBU): they are in charge of processing data received from sensors and from outside sources such as received messages from other OBUs. They also have capabilities to store, calculate and send data through available interfaces.
- Road-Side Unit (RSU): they are in charge of informing vehicles in its range by disseminating traffic conditions, meteorological or information about route condition (maximum speed, overtaking, etc.). RSUs can also play the role of a base station by relaying the information sent by a vehicle to the Public key infrastructure or central servers located in the cloud.
- Central servers: this central equipment could be a storage server, a trust entity (eg entities of the public key infrastructure) or a transaction server (eg electronic toll).
- Personal devices: devices can be smartphones, laptops or tablets.

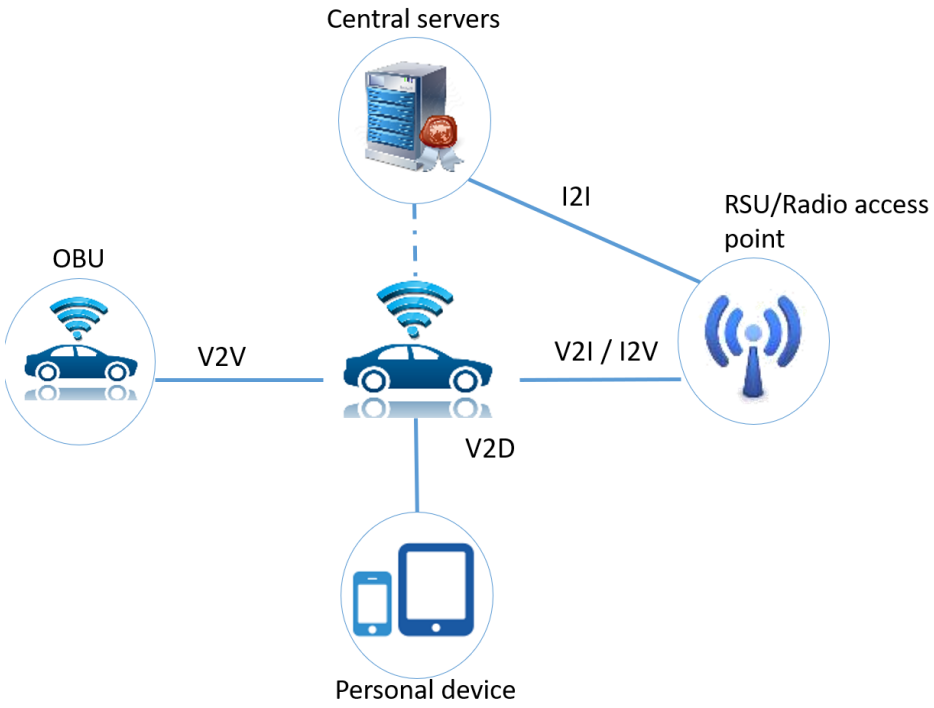

Figure 3.1: C-ITS communication entities

Vehicles (OBU), roadside unit (RSU) are called also ITS-Station (ITS-S). ITS-S communicate with each other according to several types of communications listed below and called V2X communications:

- Vehicle to Vehicle communication (V2V): V2V are generally based on IEEE 802.11p radio technology.
- Vehicle to Infrastructure communication/ Infrastructure to vehicle communication (V2I/I2V): V2I/I2V are based either on Ad Hoc communication or Cellular network such as UMTS, and LTE.
- Vehicle to Device communication (V2D): V2D are based on bluetooth or usb to interconnect the vehicle's multimedia system with the user's device (such as smartphones). The aim is to take advantage of connectivity and infotainment functionalities supported by the vehicle user's devices.
- Infrastructure to Infrastructure communication (I2I): I2I refers to communication between RSUs, and between RSU and central servers.

Vehicles can communicate with central servers via cellular or via overall (E2E) communication paths, using short-range communication link with RSUs.

3.1.2 Dedicated frequency

IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication system. It consists of an enhancements to 802.11 to

support Intelligent Transportation Systems applications. This includes data exchange between highly mobile vehicles and between the vehicles and the roadside infrastructure.

In the United States, the Federal Communications Commission (FCC) has allocated the spectrum of 75 MHz for the WAVE. The licensed ITS band in Europe is in the range of 5.9 GHz, known as ETSI ITS-G5 [9]. The spectrum frequency range is divided into 4 ranges and its usage is presented in table 3.1. ITS-G5 technology is tailor-made for road safety applications. Since ITS-G5 is a wireless technology, it can communicate beyond the line-of sight which allows dealing with the limits of the in-vehicle sensors [10]. Thanks to this broadcast technology, vehicles can communicate with each other and other relevant recipients at once. Its properties make it suitable for numerous road safety applications such as emergency brake, vulnerable road user warning or platoons. ITS-G5 is designed to operate at short-range and does not require any network infrastructure. Vehicles in the same geographic range can form an adhoc network.

The cellular standardisation organisation 3GPP is working on cellular short-range communication technologies for C-ITS. One of them, LTE-V2X, is based on 4G cellular standards. LTE-V2X is sometimes also referred to as either 3GPP 'Release 14' or 'Release 15'. The 3GPP releases 14, 15 and 16 are called C-V2X. C-V2X is a short-range communication technology and technically very different from 4G and 5G, which are long-range cellular communication technologies.

	Frequency range [MHZ]	**Usage**
ITS-G5D	5905 to 5 925	Future ITS applications
ITS-G5A	5 875 to 5 905	ITS road safety related applications
ITS-G5B	5 855 to 5 875	ITS non-safety applications
ITS-G5C	5 470 to 5 725	RLAN (BRAN, WLAN)

Table 3.1: ITS Frequency allocation in the European Union

3.1.3 Characteristics

C-ITS is a complex system that will be confronting many critical challenges for user acceptance. In this section we present its characteristics and main challenges:

- Mobility: in C-ITS the topology is very dynamic, vehicles are permanently moving. Communication environment is sometimes challenging when vehicles enter a tunnel, or in rural areas. However, ensuring a good communication and routing is a challenging task.

- Connectivity: ITS-S can enter rural areas that are not covered by network connectivity. V2V communications can be done by ITS-G5 technology. On the other hand, vehicles may need to communicate with central servers or the PKI which requires a network connectivity. The connectivity remain a good challenge in such cases. Existing solution proposes to have hybrid communication technology such as 802.11P, cellular, Wi-Fi and vehicles can use available technology in case of connectivity problem.

- High density : nodes or entities in C-ITS are the vehicles, buses, motors, etc... the number of entities can vary depending on the road topology (rural areas, down-towns, etc ...), and the time (peak hours,

late night hours, etc ...). In order to deal with this density change, a dynamic scalable solution for large scale system should be taken into account.

- Interoperability: many organizations and countries are working on C-ITS. The automobile business is not centralized in one country or one continent. It is possible for a French vehicle to be operable in another EU country. Thus, interoperability is a key challenge especially for security interoperability, such as PKI and secure communications.

- Delay-sensitive: safety-critical applications needs low latency communication and jitter (small variations in delay on packet arrival times that may have impact on real-time applications). C-ITS Safety applications are high real-time systems for distributing 'tactical' information (on which automatic decision might be taken).

- Security: exchanged information between vehicles require security protection, such as confidentiality, integrity, non-repudiation, plausibility etc. For example, vehicles shall not be able to send a message with fake position that may disturb the system. The use of the PKI is proposed as a solution for security protection. Many challenge still exist and solutions need to be improved. This thesis handles some of the security issues.

- Privacy: vehicles send periodically messages that contain information that could be directly related to driver's privacy such as position, direction, heading etc... this information can be collected and analyzed in order to create user profiles and thus track vehicles. Using pseudonym identity in the communication is a proposed solution for privacy protection but it is still not sufficient. Privacy protection remain one of the main challenges of the C-ITS.

3.1.4 Data Type Message format

Messages used in C-ITS are presented below:

- Cooperative Awareness Message (CAM): provide a basic awareness service in C-ITS networks, by periodic sending of status data to neighboring nodes with a generation rate between 1 Hz and 10 Hz. The purpose of CAMs is to allow ITS users to provide other users information about their status and environment (presence information, location, speed, heading etc.). CAMs are disseminated to neighboring ITS-S that are located within a single hop distance from the sender. By receiving CAM messages, the ITS station is aware of other stations in its neighborhood and knows their positions, movement and other relevant characteristics. A CAM is composed of one common ITS Protocol Data Unit (PDU) header and multiple containers. The ITS PDU header is a common header that includes the information of the protocol version, the message type and the ITS-S Identity (ID) of the originating ITS-S. For ITS-Ss a CAM shall comprise one basic container and one high frequency container, and may also include one low frequency container and one or more other special containers: the basic container includes basic information related to the originating ITS-S. The high frequency container contains highly dynamic information of the originating ITS-S and the low frequency container contains static and not highly dynamic information of the originating ITS-S. Figure 3.2 illustrates the structure of a CAM as specified by ETSI EN 302 637 [11].

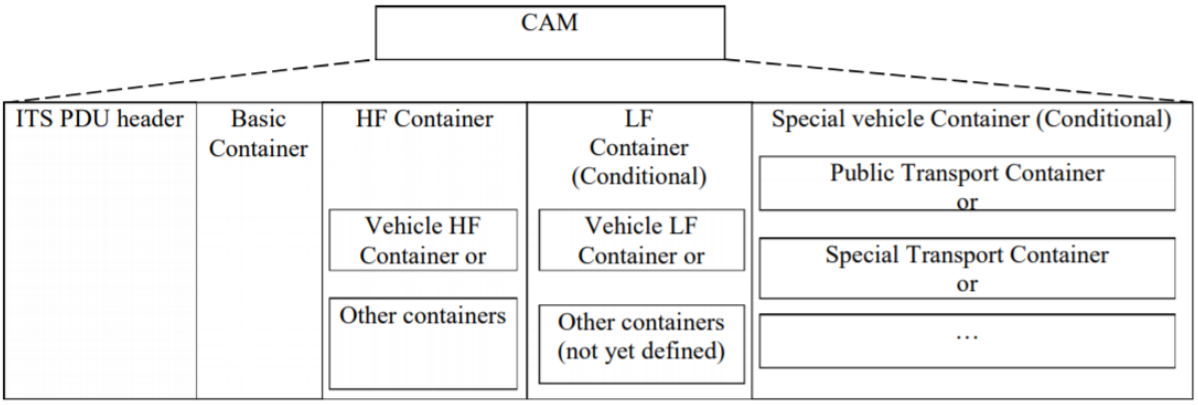

Figure 3.2: General CAM structure

- Decentralized Environmental Notification Message (DENM): referring to ETSI EN 302 637 [11], DENM contains information related to a road hazard or an abnormal traffic conditions, with its type and its position. The DEN basic service delivers the DENM as payload to the ITS networking transport layer for the message dissemination. Typically for an ITS application, a DENM is disseminated to ITS-Ss that are within a geographic area through direct vehicle-to-vehicle or vehicle-to-infrastructure communications. At the receiving side, the DEN basic service of a receiving ITS-S processes the received DENM and provides the DENM content to an ITS-S application. This ITS-S application may present the information to the driver if information of the road hazard or traffic condition is assessed to be relevant to the driver. The driver is then able to take appropriate actions to react to the situation accordingly. Figure 3.3 illustrates the structure of a DENM as specified by ETSI EN 302 637 [11].

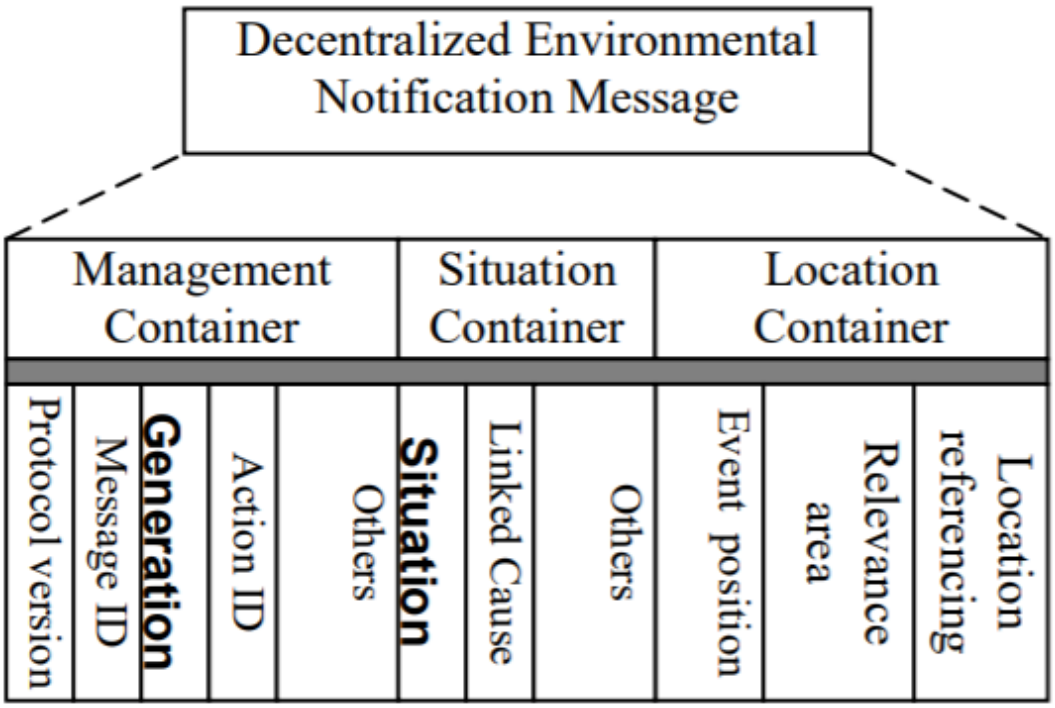

Figure 3.3: General DENM structure

- Signal Phase and Timing (SPAT): SPAT messages contain information about the current traffic light status and the time change of the traffic signal ahead, as well as, when the next signal stage change. It also provides information about approaching traffic to optimize the signal system.
- Map Data (MAP): MAP messages describe the physical geometry of one or more intersections and the associated lanes.

3.2 Security and privacy in C-ITS

In order to preserve security and privacy, a security architecture needs to be defined. ETSI and IEEE have proposed a Public Key Infrastructure (PKI) architecture to deal with security and privacy issues.

The PKI is a common infrastructure composed of entities that aim at managing, creating and distributing digital certificates. The traditional PKI architecture (e.g used for traditional internet) is composed of a Root certificate authority, a registration authority which verifies the identity of entities requesting digital certificates, and a certificate authority (CA) that stores, issues and signs the digital certificates [12] (e.g one CA has the role of delivering digital certificate). In C-ITS, the problem is that vehicles need to guarantee their privacy beside the operator. Hence, the idea is to separate the roles: an entity that registers the vehicles and another one that delivers pseudonym certificates which will be used by the vehicles to sign their messages. This ensures that none of these entities has the ability to link multiple pseudonyms certificates from the same vehicle and thus preserve vehicle's privacy. ETSI PKI is the lower layer of the ETSI Security Credential Management System (SCMS) architecture presented in the next section.

3.2.1 ETSI PKI

ETSI SCMS, presented in Figure 3.4, consists of two layers, the upper layer, the governance layer and top level entities and the lower layer which consists of PKI operational entities.

3.2.1.1 ETSI SCMS Upper Layer

The SCMS upper layer consists of:

- Trust List Manager (TLM): creates and signs the Extended Certificate Trust List (ECTL), which consists of the list of trusted Root CA's certificates and TLM certificates.
- C-ITS Point Of Contact (CPOC) : is in charge of collecting the trusted Root CAs certificates and providing them to the TLM. It also provides the ECTL to interested entities in the system.
- Certificate Policy Authority (CPA): is designating and authorizing the TLM and CPOC. It decides which Root CAs are trusted and approve/revoke Root CAs certificates in the TLM. The CPA is be composed of representatives of public and private stakeholders.

3.2.1.2 ETSI SCMS Lower Layer

The SCMS lower layer consists of ETSI PKI entities presented in figure 3.4 and described below [13]:

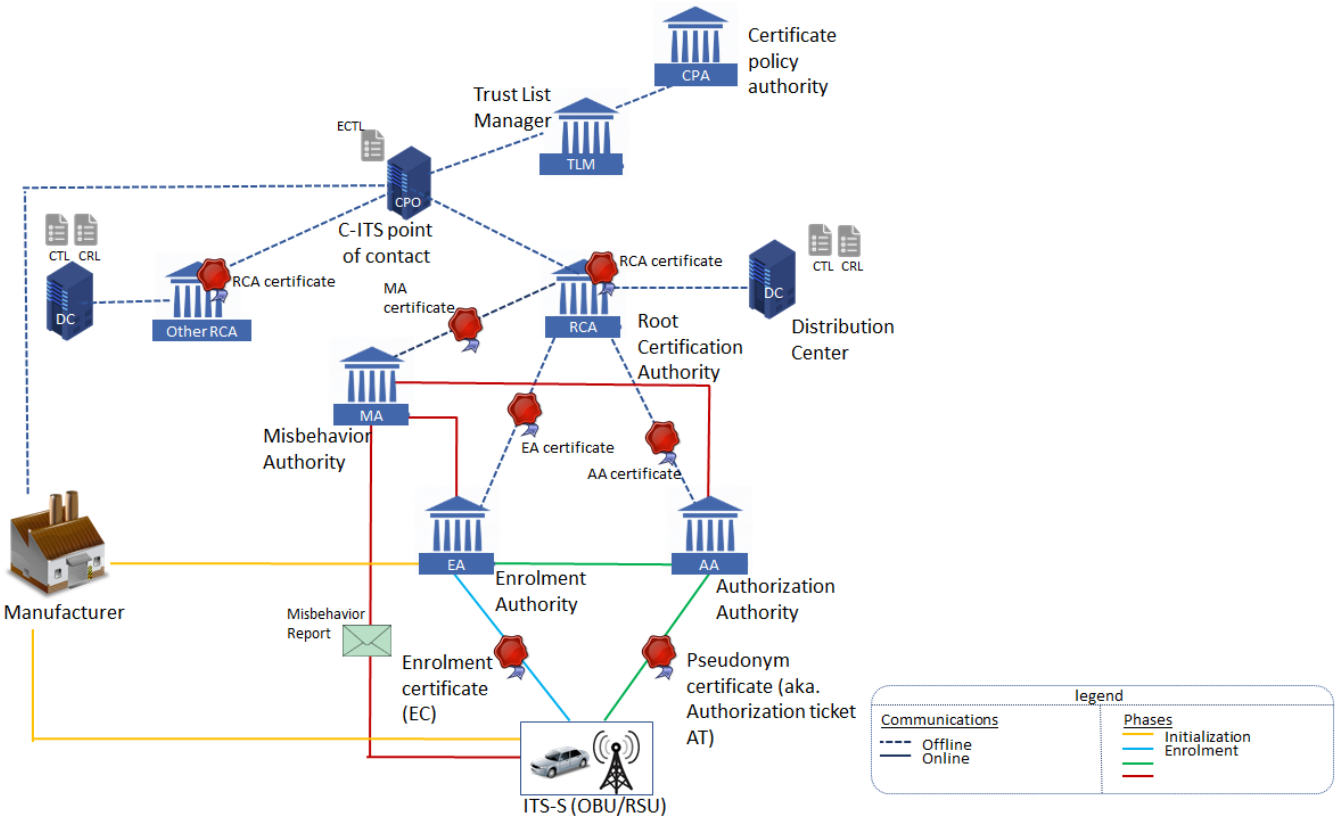

Figure 3.4: ETSI PKI Architecture

- Root Certificate Authority (RCA): RCA is the root of trust for all certificates within the PKI hierarchy. It delivers certificates to the Enrolment Authority (EA) and the Authorization Authority (AA) to authorize them to issue certificates to ITS-S.

- Authorization Authority (AA): AA issues Authorization ticket (AT) to ITS-S that are used to sign messages in V2V communications. AT are called also pseudonym certificate. The vehicles have usually a pool of valid AT that are changed during the communication to prevent tracking the vehicle.

- Enrolment Authority (EA): EA issues Enrollment Certificate (EC) for requested ITS-S. EC are considered as a proof of identity, thus used to identify and authenticate ITS-S within the PKI. They are not used in the V2V communications, they are only used to request an Authorization Ticket (AT).

- Distribution Center (DC): provides to ITS-S up-todate trust information (CRL and CTL) necessary to validate that received information coming from a legitimate and authorized ITS-S/PKI authority.

- Misbehavior Authority (MA): it is responsible for the misbehavior detection by the processing of the misbehavior reports received from vehicles.

- Manufacturer: installs necessary information for security management in ITS-S at production.

3.2.2 IEEE PKI

As presented in figure 3.5, the IEEE 1609.2 standard defines the US PKI that consists of the entities described below [14] [15]:

- SCMS Manager: is responsible for managing all other components. It insures interoperability, privacy, security and auditing of the system, and manages the activities required for operation of the SCMS.
- Root Certificate Authority (Root CA): the root of trust of the system, its main role is to produce a self-signed certificate and to issue certificates to the other certification authority (MA, LAs and RAs).
- Intermediate certificate authority (Intermediate CA) : the main role of the Intermediate CA is to protect the Root CA from direct access to the internet and decreases the amount of connection to the RCA when a new SCMS entity is added to the system.
- Linkage authority (LA): it aims at generating linkage values, which are used in the revocation process. Two LAs are considered in the SCMS are LAl and LA2.
- Location Obscurer Proxy (LOP): the main role of the LOP is to obscure the location of the On boad equipments (OBE) that intend to communicate with the SCMS components and to shuffle misbehavior reports in order to increase the privacy of the users.
- Authorization Certificate Authority: the role of the AA is to issue short term certificates and to collaborate with the MA, RA, and LA in order to identify linkage values to place on the CRL if misbehavior has been detected.
- Registration Authority (RA): the registration authority receives certificate requests from the OBE via LOP, requests and receives linkage values from the Las, and sends certificates requests to the (AA). The RA maintains a blacklist of enrollment certificates to reject any request from revoked OBE.
- Enrollment certificate authority (ECA): issues enrollment certificates, which act as a passport for the device and can be used to request pseudonym certificates. Different ECAs may issue enrollment certificates for different geographic regions, manufacturers, or device types.
- Certification services: provides information on which types of devices are certified to receive digital certificates and specifies the certification process.
- CRL Store (CRLS): the Certificate revocation list (CRL) stores and distributes CRLs. This is a simple pass-through function since CRLs are signed by the CRL Generator.
- CRL Broadcast (CRLB): it broadcasts the current CRL, may be done through Road Side Equipment (RSEs) or satellite radio system, etc. This is a pass-through function.
- Device communication manager: provides authenticated information about SCMS component configuration changes to devices, which may include a component changing its network address or certificate, or relaying policy decisions issued by the SCMS Manager. It is also used to attest to the Enrolment CA that a device is eligible to receive enrolment certificates.

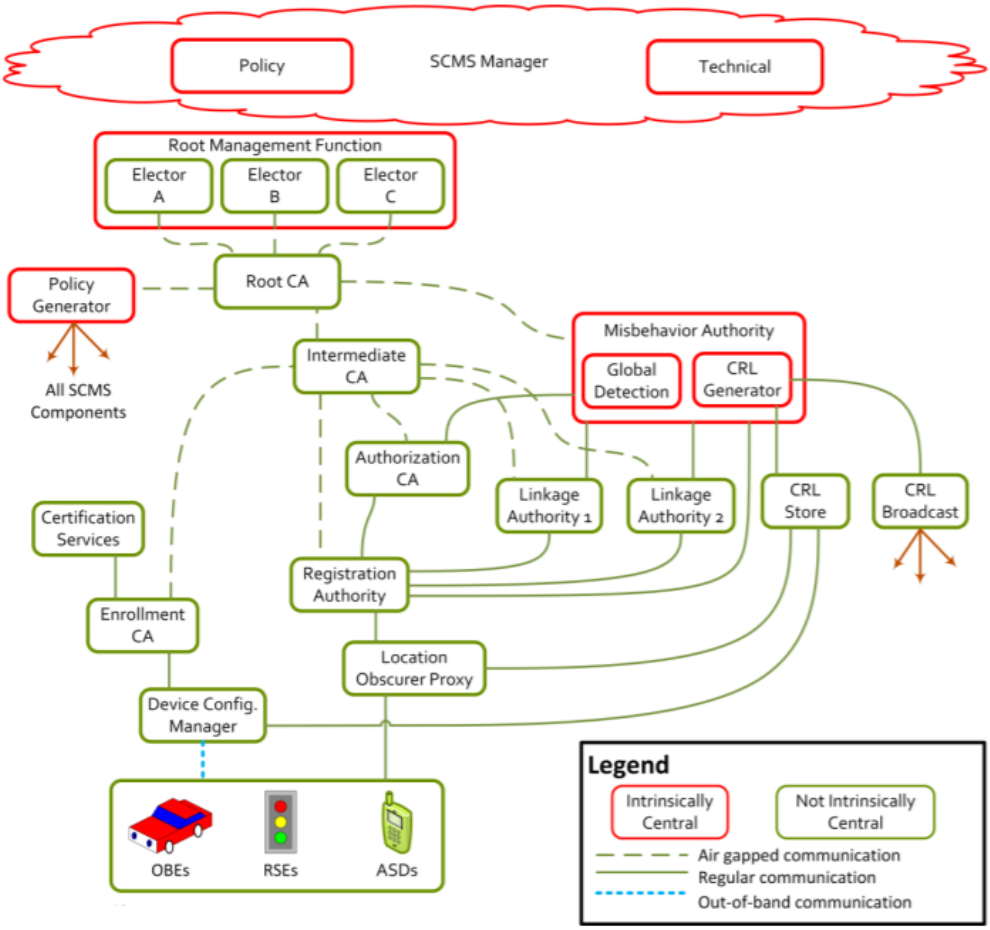

Figure 3.5: IEEE PKI architecture

- Misbehavior Authority (MA): processes misbehavior reports to identify potential misbehavior by devices, and if necessary revokes and adds devices to the CRL. It also initiates the process of linking a certificate identifier to the corresponding enrolment certificates, and adding the enrolment certificate to an internal blacklist. The MA contains two subcomponents:
  - Global Detection (GD): determines which devices are misbehaving.
  - CRL Generator (CRLG): issues certificate revocation lists to the outside world.

3.2.3 Comparison of EU and US PKI architectures

European and American architecture are different in terms of entities. As presented in the section above the US PKI entities are more numerous than those in EU. This is because some functionalities are regrouped in one entity in EU PKI. Table 3.2 presents a comparison of EU and US PKI.

	EU PKI	**US PKI**

Misbehavior detection	Ongoing subject (the architecture including the MA is in a pre-standardization phase)	Misbehavior reports are processed by the Misbehavior authority (MA) to identify potential misbehavior by devices, and if necessary, revokes and adds devices to the CRL. The MA also initiates the process of linking a certificate identifier to the corresponding enrolment certificates, and adding the enrolment certificate to an internal blacklist.
Publication of revoked entities	The distribution center broadcasts the Certificate revocation list (CRL) to the ITS-S.	CRL store and CRL broadcast are responsible for the revocation list
Pseudonymity of user identities	Authorization authority issues pseudonym certificate to the requesting ITS-S	Authorization certificate authority issues pseudonym certificate to the requesting ITS-S
Long term certification	Enrollment authority is responsible for issuing a long term certificate (e.g enrollment certificate) that is used to request multiple pseudonyms certificate	Enrollment Certificate Authority is responsible of issuing a long term certificate (e.g enrollment certificate) that is used to request multiple pseudonyms certificate
Root management	Certificate policy authority decides if root CAs are trustable and approves/removes the Root CAs operation in C-ITS trust domain by notifying the Trust List Manager (TLM) about approved/revoked Root CAs certificates	Electors vote if the root can be revoked or added when SCMS detected a compromised root

Table 3.2: EU PKI vs US PKI

3.2.4 Security Requirements in C-ITS

Some security and privacy requirements should be addressed in the context of the C-ITS, even though the requirements importance level depends on the application it self, this means that some applications such as sending a pseudonym certificate request to the PKI, need a high level of confidentiality, on the other hand sending a CAM message does not need any confidentiality restriction. The level of the security and privacy requirements for each application is studied in chapter 4 of this thesis. In this section we give a general definition of all the security and privacy objectives:

- Availability: ensures timely and reliable access to data and the system. It is crucial especialy for safety applications.

- Authentication and Authorization: authentication ensures that the entities involved in the communication are correctly identified and authenticated. An authorization entity is necessary for the applications that need the definition of the rights that an ITS-S (vehicle or infrastructure) has.
- Integrity: ability to protect each message sent from modification, insertion, reordering, or replays.
- Confidentiality: ensures that data access and disclosure for authorized users/devices only.
- Non-repudiation: it may be crucial in some cases (such as wrong information that causes accident) not only to identify the sender, but also get the proof from the originator of the message (for accountability).
- Plausibility: evaluating if the data included in the message is realistic or not.
- Traceability: the capability of keeping track of a given set or type of information to a given degree.

3.2.5 Privacy Objective

In general, privacy can be defined as the ability of an individual or group to control and define what information related to them can be collected and stored and by whom and to whom that information may be disclosed. The right to privacy is vital as acknowledged by The Universal Declaration of Human Rights and the European Convention on Human Rights. However, the right to privacy is becoming more and more threatened with the evolution in the field of information and communications technologies, especially for connected vehicles where huge amounts of potential personal information are processed. To deal with the privacy protection, it is possible to take a legal approach on the problem. As an example, the European Parliament and Council made the EU General Data Protection Regulation (GDPR), which aims to give a legal framework to protect the privacy of individuals on a European level, by giving control to individuals over their personal data and unifying the regulation within the EU. This regulation has tremendous implications on several areas, and in particular on C-ITS given the important volume of personal data that is processed in this context.

In parallel to the legal approach, it is possible to rely on privacy-preserving techniques and technologies. The issue of privacy has been widely researched by the scientific community, and several privacy-preserving techniques have been proposed.

- Anonymity: a system provides anonymity of a subject if the subject is not identifiable within a set of subjects (the anonymity set). In an anonymous V2X communications system, identifying the communicating units shall be impossible.
- Unlinkability: unlinkability of two or more items of interest (subjects, messages, actions ...) from an attacker's perspective means that within the system, the attacker cannot sufficiently distinguish whether these items of interest are related or not.
- Unobservability: unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. It requires

that users and/or subjects cannot determine whether an operation is being performed. Unobservability is a stronger property than anonymity, which means that if we have unobservability then we have anonymity.

- Pseudonymity: pseudonymity is the use of pseudonyms as identifiers. A pseudonym is an identifier of a subject other than one of the subject real names. In the context of ITS, pseudonymity is done with the use of pseudonym certificates. This is the main technique used to protect the privacy of ITS users.

3.2.5.1 Privacy Techniques in C-ITS

Vehicles in C-ITS exchange beacon messages such as Cooperative Awareness Message (CAM) or messages to indicate a problem on the road such as Decentralized Environmental Notification Message (DENM). These messages raise privacy issues since it becomes easy to track a vehicle and potentially retrieve information on user's position, trajectory and destination, which allows to infer information about users and their habits, their homes, their places of work, etc. This is devastating for the individual's privacy therefore, privacy preserving techniques should be used with the messages exchanged. It is also valid for messages that are not necessarily safety related such as infotainment or service-related messages. Two privacy preserving methods are presented bellow, the difference between these methods is presented in table 3.3.

- Pseudonym certificate: in the asymmetric cryptography the ITS-S generates a key pair (private key, public key) and sends the public key to the Authorization Authority (AA) in order to certificate this key. The AA validates whether this ITS-S is already registered in the Enrollment Authority (EA) and generates a pseudonym certificate for the ITS-S. Pseudonym certificates (i.e. Authorization Tickets) are used by the ITS-S to sign V2X messages. ITS-S changes its pseudonym based on a strategy that should be defined in order to make pseudonym linkage or tracking much more difficult.

- Group signature (GS): common digital signature such as Rivest-Shamir-Adelman (RSA), Digital Signature Algorithm (DSA), etc. can be used with pseudonym scheme to authenticate the messages. Group signature was first introduced by Cham et.al [16], it is a technique to achieve anonymous authentication in vehicular network without the need of pseudonym certificates. The concept of GS is to consider that it is enough for a verifier to know a message was signed by a legitimate user, without particular user signed it. An example of GS application is for keycard access to restricted areas where it is inappropriate to track individual employee's movements, but it is necessary to restrict certain areas to only employees in the group. A centralized entity chooses a public key system, gives each user a list of secret keys and publishes the complete list of corresponding public keys (in random order) in a Trusted Public Directory. Each person can sign a message with a secret key from his list, and the recipient can verify this signature with the corresponding public key from the public list. Each key will be used only once in order to ensure unlinkability. The centralized entity knows all the lists of secret keys, so that in case of dispute, he knows who made the disputed signature. Hence the centralized entity is needed for the setup and for opening a signature. Many schemes of

the group signature exist in [16]. It consists of improving the group signature by limiting the centralized entity to have all access on the secret keys. The improvement can be done by using blinded signature.

Privacy schemes

	Pseudonym certificate	**Group based signature**
Description	The Authorization Authority issues pseudonym certificates for ITS-S. The vehicle signs messages with the private key corresponding to the certified public key.	The centralized entity or group manager sends list of private keys to each ITS-S and publishes public key associated to these private keys in a public list. The ITS-S sign messages on behalf of the group. The receiver ITS-S uses the public list to verify signature
Advantages	ITS-S generates its own private and public keys and certifies them by a trusted entity	No need to have a trusted entity
Drawback	Privacy depends on used pseudonym change strategy	Hard to manage groups in a highly mobile environment Misbehavior detection
Authentication	Yes	Yes
Anonymity OBU to trust entity	Trust entity in the pseudonym scheme is the PKI (AA). The ITS-S guarantees its pseudonymity thanks to the separation of two entities EA and AA, where the pseudonym request is divided into two parts, one is encrypted with the EA public key and the other is encrypted by the AA public key	Identifying the actual signer is possible by the centralized entity or the group manager
Anonymity OBU to OBU	Using a pseudonym scheme, the ITS-S guarantees its anonymity because it does not use its real identity in the communication with other vehicles	Anonymity is guaranteed since the vehicle does not use its real identity

Unlinkability OBU to PKI	The unlinkability between the message sent between the OBU and the AA is guarantee by changing pseudonyms and all addresses (IP, MAC etc...)	The unlinkability is not guarantee as the group manager distribute the private keys, it have the link between all the private keys for a specific ITS-S
Unlinkability OBU to OBU	The linkability between sent messages depends on the used pseudonym change strategy	The linkability depends on the message content
Pseudonymity	ITS-S uses pseudonym identities in the communication, study of the of this solution is detailed in this the chapter 6	Solution dos not ensure pseudonymity of communicating ITS-S

Table 3.3: Comparison of privacy schemes

3.2.6 Standardization activities in C-ITS

The C-ITS domain is known by the large number of car manufacturer. In order to ensure interoperability, a common ITS-S communication architecture need to be defined. Many consortium such as Car2car communication Consortium [17], Vehicle Safety Communications Consortium (CAMP) and standardization groups such as ETSI, ISO, and projects such as Secure Cooperative Autonomous project (SCA) and SCOOP have contributed to the standardization activities in the C-ITS domain. In this section, we present ETSI (EU) and IEEE (US) communication architecture.

3.2.6.1 ETSI ITS-S Communication Architecture

The ETSI ITS-S communication architecture is described in ETSI EN 302 665 standard [18]. It follows the principles of the OSI model [19] for layered communication protocols is extended for inclusion of ITS applications. As presented in figure 3.6 ETSI's communication architecture consists of four horizontal layers: access, networking/transport, facilities and applications layers and two cross layers: security and management layers. Each layer provides the following functionalities:

- Access layer: it manages the access external or internal interfaces and access technologies that are available in the ITS-S either wired or wireless (802.11p, Cellular etc...)
- Networking and transport layer: it provides data transport between source and destination ITS-S. ETSI considers the following communication profiles to achieve this task: BTP [20] over GeoNet [21], TCP/UDP over IPv6 and TCP/UDP over IPv6 over GeoNet [22].
- Facilities layer: it provides support to ITS applications by sharing generic functions and providing three types of services such as [23]:

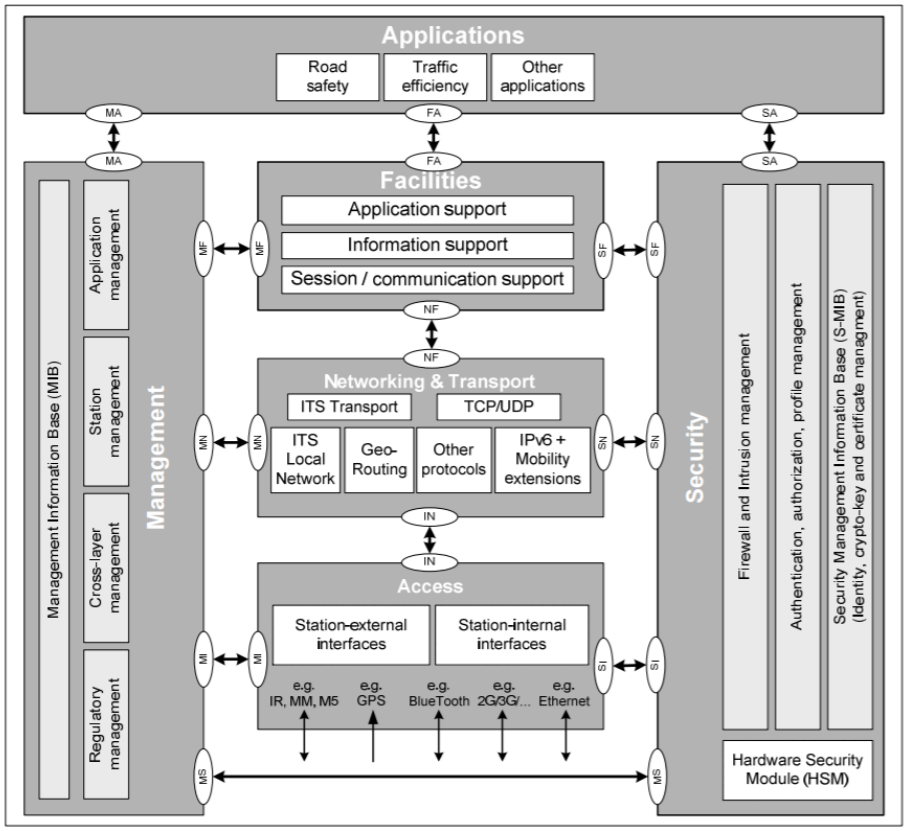

Figure 3.6: ETSI communication architecture

1. Application support: it provides common features and services for the execution of the applications. An example feature of this layer is the management of CAMs and DENMs.
2. Information support: it provides common data and database management functionalities for application execution.
3. Session/communication support: it provides services for communication support such as addressing mode, geocasting support and session support.

- Applications layer: runs one or more applications presented in chapter 4.
- Management cross layer: it manages the access, networking and transport, and facilities, depending on the application layer requirement.
- Security cross layer: it provides security services to all communication stack layers.

3.2.6.2 IEEE wireless access in vehicular environments (WAVE) Communication Architecture

The IEEE WAVE communication architecture is defined in [24]. It is structured in two main planes and some services presented in figure 3.7 and described below:

- Physical and WAVE MAC layer: the two sub-layers construct the lower layer of the WAVE model. They provide some features such as channel timing and switching, MAC-layer readdressing in support of pseudonymity etc..

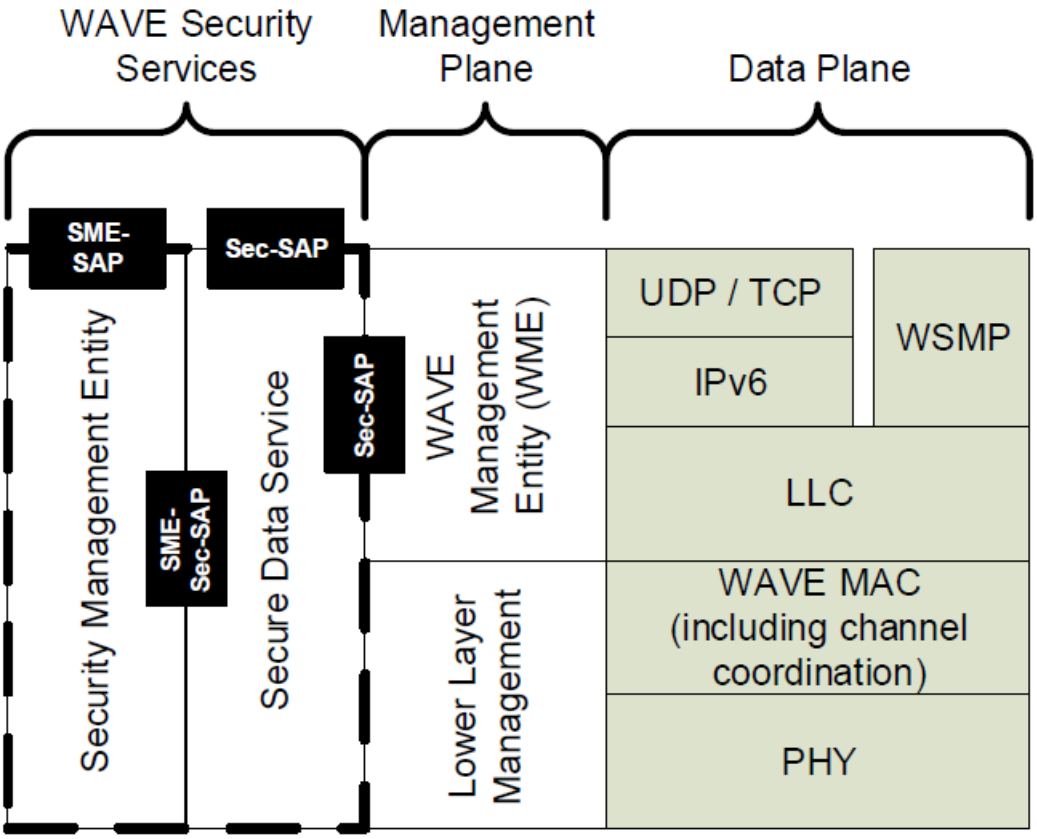

Figure 3.7: IEEE WAVE reference model

- Logical Link Control and WSMPlayer: the two sub-layers construct the upper layer of the WAVE model. It provides service advertisements and channel scheduling, WAVE short message protocol. It defines a protocol for WAVE communication. TCP/UDP over IPV6 are supported.
- Management layer: provides management services such as over-the-air management.
- WAVE Security Services: specifies communications security for WAVE Service Advertisements and WAVE Short Messages and additional security services that may be provided to higher layers.

3.3 Attacks

In this section we present the attacks types in C-ITS.

3.3.1 Attack types

Like any other type of systems, C-ITS is exposed to multiple types of attacks. Many works in the literature investigate on possible attacks.

In [1], authors present a classification on possible attacks in a vehicular network. The classification, described below and depicted in figure 3.8, is based on the security objective (Confidentiality, integrity,

etc) the attack can harm.

- **Attacks on Availability**: in [25] Houmer et al. present an attack tree for VANET availability (e.g investigation in the attacks on the availability in vehicular network). They consider three ways to do an attack on availability: 1)Black Hole consists of traffic redirection, 2) Denial of Service consists of making the network unavailable for valid and legitimate users, 3) Malware/ Spam consists of creation of a virus or malware for the purpose of harming a computer system to send bulk messages indiscriminately.

  BlackHole attack occurs by cheating the routing protocol and establishing a forged route. The attacker drop traffic incoming or outgoing without denouncing the source that the data did not attain its destination.

  Denial of Service (DoS) occurs by dispatching wrong messages on the network which is called channel jamming. Also by executing the ping tool, an ICMP echo request packet is sent to the target computer. The return IP address of the ping packet is established from the IP address of the target computer. The ping is sent to all broadcast IP address. Each computer responds to a simulated ping packets and responds to the target computer, which is then saturated, that is called smurfing. DoS can also occur by Flooding, which means sending large amounts of traffic.

  Malware/ Spam occurs by inserting a copy of malicious code into a reliable program and becoming part of it. The malware send spam messages (junk messages), the attacker consume the quota available through a service and then prevent you from receiving legitimate messages.

- **Attacks on Confidentiality**: vehicles exchange periodically V2X messages that contain kinematic information of the vehicle. Messages eavesdropping is a challenge in vehicular network, attackers can be a vehicle (stopped or in movement), someone disposing a physical antenna that receives and gathers all exchanged messages within an area.

  Social attacks are also confidentiality critical attacks [26], The basic idea of the attack is to confuse the victim by sending unethical and unmoral message so that the driver gets disturbed. The legitimate user reacts in an annoyed manner after getting such kind of messages which is the main objective of the attacker. Usually this type of attacks can be prevented by increasing sensitization of the user's on social engineering techniques [27].

- **Attacks on Integrity and data trust**: some safety applications require multi-hop communication. Message suppression can be critical for this type of applications and could disturb the system especially in case of suppression of safety messages. [28] [27].

  Another type of attacks on integrity. An attacker can fabricate messages, or warnings and send them into the network [29].

- **Attacks on Non-repudiation**: non-repudiation aims to avoid one entity to deny having made some action. In the existing architecture,vehicles use digital signature to guarantee the non repudiation.

- **Attacks on Authenticity/authorization**: Sybil attack is one of the most challenging attacks in vehicular network. It occurred due to capacity of the vehicle to send multiple messages with different

pseudonym identities. More precisely, vehicles have a pool of valid identities (e.g pseudonym certificates) that can be used to sign V2X messages. It is possible that an attacker creates multiple messages with fake information and signs them by using its valid pseudonym certificates. Receiver of messages will consider two or multiple vehicles in the road, which is not the case. This attack can disturb system's safety.

Another example of attacks on authenticity is the GPS spoofing [30]. The global position system (GPS) provides accurate location information to users all around the world. In vehicular network, GPS information will be used by safety applications. However, as the GPS signal has no encryption or authorization mechanism and the detailed information about GPS signal is open to the public, it is feasible for an attacker to generate fake GPS signal. Victims may receive fake information about timing, location etc ..

Privilege escalation threats impact authorization that is considered when an attacker potentially gains privileged access by changing their roles and restrictions [15]. This attack can be used when attacker tries to inject malicious code on an in vehicle board unit and needs an elevation privilege to run his malicious code.

We believe that this classification is interesting in order to categorize the possible attacks. In this thesis, we will study attacks on pseudonimity aspects of vehicular networks (e.g attacks came from the use of pseudonym certificate). Detailed risk analysis is presented in chapter 5.

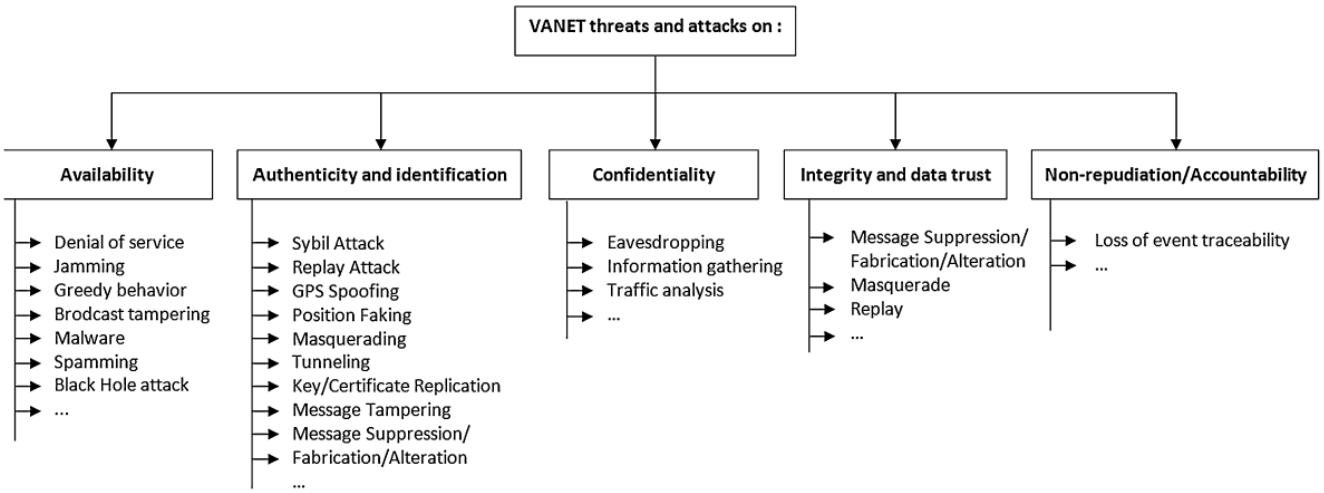

Figure 3.8: Examples of VANET threats and attacks from [1]

3.3.2 Attacker Model

Attacker model specification is a process used to identify potential threats from a hypothetical attacker's point of view. The purpose of attacker model's specification is to provide defenders with a systematic analysis of the probable attacker's profile, and the most likely attack vectors. Nowadays, the attacker model depends on a specific problem (e.g attacker models for routing protocols), Most of these models were not proposed for general use.

Attacker models are crucial in vehicular network. They are used to find the weak vectors of the system. They can be constructed by varying number of capabilities or goals. In [2] Martini et al. consider 3 factors that can be used to construct an attacker model. Factors are presented in figure 3.9 and described below:

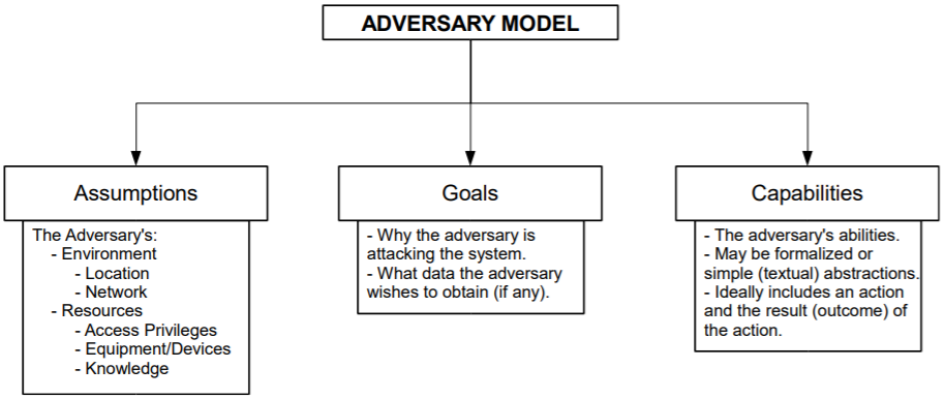

Figure 3.9: The components of our adversary model definition from [2]

- Adversary assumptions: it depends on the attacker environment and resources. For example, an adversary could be external to a system or internal and may have privileged access on a network or data of the system. For resources, the same attack can be performed differently depending on the assumptions. An attacker with full access privilege on the system will perform more successful attacks than an attacker with partial access. Same for the equipment and knowledge holded by the attacker.

- Adversary goals: the attacker's goal may be financial gain such as tracing user's profile and selling the traces in case of tracking attack for example. Another goal can be to direct traffic away from his home in case of Sybil attack. In worst case, the goal of the attacker may be to disturb the system for evil reasons.

- Adversary capabilities: it consists of the interaction between the attacker and the secure system. A number of commonly used attacker capabilities are as follows: Send, Reveal and Execute. Another commonly used adversary capability is the Corrupt capability, which allows an adversary to take control of a target and learn its internal state an extremely powerful capability, and one that allows the modeling of a malicious insider within a system

Another factor presented in [31] by Boualouache et al. is the attack time duration. It consists of the duration of the attack, it can be:

- Short-term attack duration: it consists of a successful attack for a couple of seconds. This feature importance is very related to the attack, for example in case of tracking attack, the more time the attacker can track a vehicle the more successful the attack is.

- Mid-term attack duration: it consists of a successful attack for a couple of hours.

- Long-term attack duration: it consists of a successful attack for days or months. For example, in case of tracking attack, the attacker is able to link different sets of location samples from different trips.

Petit et al [32] pointed out that due to the cost of eavesdropping the global coverage, is almost impossible to be achieved. They defined more realistic adversary called mid-sized adversary. The adversary can cover an area larger than a local passive adversary and less than a global passive adversary. In another words, it can cover a limited number of areas without getting the full coverage.

ETSI proposes an attacker model in [33] for the vehicular network, it takes into account time to do the attack, expertise, knowledge of the attacker, opportunity, and equipment needed to do the attack. More details about the attacker model are presented in Chapter 5.

3.3.3 Attacker's types

In [32], Petit et al. consider that an attacker can be :

- Global vs. Local: compared to a local attacker, a global attacker has an overall coverage of the VANET. It can eavesdrop all exchanged messages between vehicles, or between vehicles and PKI.
- Active vs. Passive: an active attacker can alter or inject messages. A passive attacker can only eavesdrop messages.
- Internal vs. External: an internal adversary is an authenticated member (e.g has a valid key materials). An external adversary is considered as an intruder.
- Malicious vs Rational: the malicious attacker aims to harm the entity or the system functionality. A rational attacker attempts to gain profit and personal advantages.

3.4 Projects on C-ITS

Multiple projects in the world are working on C-ITS security and privacy aspects. In this section, we will present three European projects:

3.4.1 Secure Cooperative Autonomous systems (SCA) project:

SCA project was launched in July 2017 by the IRT SystemX and the participation of multiple industrial partners such as Groupe Renault, Groupe PSA, IDnomic, Oppida, Transdev, Trialog, Valeo, YoGoKo, and an academic partner Institut Mines-Télécom.

The main objectives of the SCA project are the analysis of innovative autonomous vehicle use cases, study of the system evolution capability and its crypto-agility, security assessment and penetration tests, improving communication systems interoperability, and scalability and dynamic dimensioning of the C-ITS PKI. SCA follows on from the ISE project (ITS SEcurity), completed in June 2017, which led to the development of the public key infrastructure for cooperative ITSs. SCA participates and contributes in multiple standardization activities such as ETSI and Car2Car communication consortium.

The work of this thesis is conducted within the context of ISE and SCA projects. I participated essentially in the use case study, security assessment and performance evaluation of security system.

3.4.2 SCOOP

Système COOpératif Pilote (SCOOP), is a pilot project for and the first C-ITS deployment project in Europe. It started in 2014 (phase one) and ended in 2019 (phase 2). In France, this project is managed by the French Ministry of Transport. The main objectives of SCOOP project are: Improving road safety, making traffic management more efficient and contributing to C02 emission reductions, optimizing infrastructure management costs, and preparing the vehicle of the future and developing new services or applications for connected vehicles. To achieve the objectives, French partners aimed at SCOOP aims at deploying informative use cases in 3000 vehicles (Renault vehicles, PSA vehicles, and road operator vehicles) over 2000 km of roads, on in five French sites : Ile-de-France, Paris-Strasbourg highway, Isère, the ring road of Bordeaux, and Bretagne. These sites are characterized by a great diversity of road types (motorways, structuring roads in the metropolitan area, bi-directional interurban and local roads).

SCOOP french and EU partners are: Ministry of the Environment, Energy and Sea, Department of Isére, Agglomeration of Saint-Brieuc, departments of Côtes d'Amor, Ille et Vilaine, Brittany Region, represented by ITS Bretagne Direction of roads Ile de France DiRIF, Interdepartmental Directorate of Atlantic Roads DIRA ,Interdepartmental Direction of Roads West DIRO, Sanef, Groupe PSA , Groupe Renault, Cerema, IFSTTAR, GIE Renault-PSA, Université de Reims, Institut Mines-Telecom ParisTech, Orange, IDnomic, and many foreign partner such as DGT Ministry of the Interior, CTAG - Automotive Technology Center of Galicia from Spain. Institute for Mobility and Transport IMT, Portugal Estradas, Brisa, Auto-Estradas Norde Liberal AENL from Portugal and ASFINAG from Austria.

3.4.3 Connected Corridor for Driving Automation (CONCORDA)

CONCORDA project contributes to the preparation of European motorways for automated driving and high density truck platooning with adequate connected services and technologies. CONCORDA project was launched in October 2017. Its main role is the preparation of European motorways for connected and automated driving and high density truck platooning, by providing adequate connected services and technologies in terms of interferences and interoperability. Many European countries are implied in this project such as Austria, France, Germany, Greece, Italy, Netherlands, and Spain.

3.5 Conclusion

In this chapter we first presented C-ITS communication entities, type of communications and environment characteristics, and message types and format. We then presented the security point of view in C-ITS, we described ETSI and IEEE PKI architecture, we detailed the role of each entity in these two architectures. We compare ETSI and IEEE PKI architecture. We presented the privacy problem and the existing privacy preserving techniques and we compared them. We precise that in this thesis we use the pseudonym scheme which is compliant with ETSI adopted scheme. We presented then ITS-S communication architecture in ETSI and IEEE standards. Finally, we presented possible attacks classification based on what

security objective the attack can harm. In this thesis, we propose to extend this classification and focus on the attacks on pseudonymity aspects.

Chapter 4

Use case study

Use case is a specific situation in which a service could potentially be used. In C-ITS, many use cases (UC) exist in the literature such as Map update, collision warning, and stationary vehicle warning etc. In this chapter, we present related work on existing use cases in standards, projects, and working groups. We analyze the existing UC, we propose new ones and we finally, classify them based on criteria that we have defined. Our aim is to select some UCs that will be used in the rest of this thesis to apply risk analysis on them.

4.1 Related works

In Europe, ETSI TR 102 638 [34] details the Basic Set of Applications (BSA) which consists of a list of use cases considered for Day-1 deployment (i.e. use cases that may be deployed simultaneously at a targeted time). The selection of use cases presented in table 4.2 and 4.3 is proposed by the different participants at ETSI standard. Most of use cases included in ETSI are application level.

In the US, standardization specifies use cases that are more related to security and privacy. Whyte el.al [14] present the US security system for C-ITS, namely Security Credential Management System (SCMS). SCMS defines the following classes of use cases related to security: pseudonym certificate provisioning, misbehavior reporting, misbehavior detection and revocation. We added those UCs to table 4.2 and 4.3 that regroup all UCs from the literature.

With the ongoing development of 5G and the Device-to-Device (D2D) communication, the cellular technology tends to become a strong candidate for V2X communications. In order to deal with new and complex situations and needs, projects and industries introduce the 5G technology on vehicular network, especially to improve performances [35]. The 5G PPP presents in [36] its vision on how 5G will enable the next generation of connected and automated driving and new mobility services. They also provide new use cases on which 5G communication would be required such as automated overtake, high density platooning and see through sensoring. Those use cases are added to table 4.2 and 4.3 .

Over the last decade many European projects have been conducted (SEVECOM, COMeSafety, EVITA, Drive C2X, PRESERVE, SCOOP@F, ...). These projects contribute to the C-ITS by proposing and studying various use cases. Some of these use cases are already integrated in the European standards

whereas others are not. Some of the latter are described in section 4.2

Sjoberg et.al [37] present two classes of applications: *Day one* and *Day two and beyond* applications. The *Day one* UCs are driver support functions that intend to increase information horizon of the driver. On the contrary the *Day two* UCs, focus on more advanced applications designed for automated driving.

The current literature is full of C-ITS use cases that focus on road safety, traffic efficiency and driver assistance for either connected and/or fully-automated vehicle. However, the security and privacy aspects of C-ITS communication is much less considered especially in European standard in which we participate and contribute. Security and privacy mechanisms indeed have specific operational requirements. That is why use cases that are oriented to security and privacy needs also have to be defined and considered. This is the purpose of the first contribution. We propose and describe new use cases that are of paramount importance to ensure that security and privacy functions work properly. We proposed those use cases to be added to the revised version of ETSI TR 102 893 [38], the proposition was accepted to be published in the future.

In this chapter, we first make an inventory of the existing use cases from European and American standardization bodies, the cellular community and European projects. We then propose new use cases, mostly related to security and privacy aspects, that are not considered yet. Finally we propose a classification methodology based on the K-means clustering method to classify those use cases. We then use the methodology on the use cases by using security and technical criteria for classification.

4.2 Use case description

In this section, we describe the existing use cases regrouped from the literature (related work section). Table 4.2 and 4.3 present the source of each use case (ETSI, EU projects, US, literature) and the analysis of each use case based on criteria proposed in table 4.1.

- **Slow vehicle indication**: slow vehicle signals its presence (vehicle type) to other vehicles to contribute in the improvement of the traffic fluidity.
- **Emergency vehicle approaching**: active emergency vehicle indicates its presence. In many countries the presence of an emergency vehicle imposes an obligation for vehicles in the path of the emergency vehicle to give way and to free an emergency corridor.
- **Across traffic turn collision risk warning**: to inform approaching vehicles that a vehicle (the transmitting vehicle) is intending to turn across traffic.
- **Merging traffic turn collision risk warning**: provide information of presence, position and movement of incoming vehicles from left side, turning right.
- **Co-operative merging assistance**: the vehicles involved in a merging negotiate together the merging process to avoid collision.
- **Intersection collision warning**: informs vehicles in a risk of collision at an intersection in order to avoid the collision between vehicles.

- **Co-operative forward collision warning**: it is based on co-operation between vehicles which detect a risk of forward collision. Such co-operation is achieved to avoid accident.
- **Lane change maneuver**: provides the driver assistance by giving information about vehicles on the neighboring lane and facilitating this change through V2V co-operation.
- **Emergency electronic brake lights**: it consists of vehicle signaling hard breaking to its local followers. It warns all following vehicles of a sudden slowdown of the traffic so limiting the risk of longitudinal collision.
- **Wrong way driving warning**: indicates to vehicles in the affected area that a vehicle is driving in a wrong direction in order to avoid frontal collision.
- **Stationary vehicle**: it consists of signaling that a vehicle being dangerously immobilized on the road (accident, a breakdown or any other reason) to alert other approaching vehicles of the risk to manage their navigation.
- **Traffic condition warning**: it allows any vehicle or roadside station to signal to other vehicles the current traffic condition. Such data can be used to mitigate the impact of the traffic condition on traffic flow by reducing congestion.
- **Signal violation warning**: it allows the road operator to signal to vehicles that a vehicle has violated a road signal and increased the risk of an accident. It can also be reported to appropriate authority.
- **Roadworks warning**: road operator provides information on current roadwork and associated constraints.
- **Weather information**: it consists of the capability of collecting road weather data from connected vehicles and using that data, by traffic controlling center, to develop short term warnings that can be provided to individual motorists in a specific area.
- **Decentralized floating car data**: it consists to detect and signal to other vehicles some local danger or some traffic flow evolution.
- **Vulnerable road user warning**: RSU provides warning to vehicles of the presence of pedestrian or cyclist, in case of dangerous situations.
- **Pre-crash sensing warning**: exchange of vehicles attributes to mitigate the impact of an imminent and unavoidable collision.
- **Co-operative glare reduction**: it enables a vehicle to automatically switch from high-beams to low beams when detecting a vehicle arriving in the opposite direction.
- **Motorcycle approaching indication**: it warns drivers of arriving motorcycles.
- **Safety function out of normal condition warning**: it consists of detecting a safety function (steering, braking, etc.) condition that may present dangers to other vehicles.

- **SOS service**: An SOS alarm generated automatically or manually by a customer requesting assistance to form a service center in case of life threating emergency.
- **Car rental/sharing**: a RSU which has the capability to manage the configuration of non assigned vehicles upon request from a customer and the release of returned vehicles after collecting vehicles' reports. Usage: Car rental/car sharing management.
- **Overtaking vehicle warning**: a vehicle planning to overtake another vehicle signals its action to vehicles in its range to secure the overtaking situation.
- **Co-operative adaptative cruise control**: it consists of obtaining lead vehicle dynamics and general traffic ahead in order to enhance the performance of current ACC.
- **Traffic light optimal speed advisory**: it allows a traffic light to broadcast time remaining before switching between green, amber, red) to vehicles in the road.
- **Traffic information and recommended itinerary**: RSU informs the approaching vehicles of some traffic abnormal conditions and issues recommendations in case of traffic jam.
- **Public transport information**: Service provider broadcasts information about time of buses, trains etc ...
- **In-vehicle signage**: RSU broadcast information on current valid traffic signs to the drivers .
- **Electronic toll collect**: RSU control toll collection before the access of a vehicle on a part of the road.
- **Point of interest notification**: Central entity informs vehicles about the presence of locally based services such as hotels with the opening hours, prices, waiting time, available rooms etc
- **Stolen vehicle alert**: it consists of broadcasting alerts by stolen vehicles to indicate an emergency.
- **Fleet management**: RSU provides to vehicles, some fleet management data.
- **Highway automation system**: it consists of vehicles operating as a platoon on a highway or specific lane.
- **Regulatory/contextual speed limits notification**: RSU broadcasts the current local speed limits (regulatory and contextual).
- **Map download and update**: a RSU broadcasts maps/map elements to provide efficient navigation.
- **Data provisioning**: RSU provides information about vehicle's parameters such as application names/pseudo and some keys needed for the communication.
- **Cooperative perception**: vehicles share their information gathered by their local perception sensors.

- **Longitudinal collision risk warning**: longitudinal collision refers to the collision between vehicles (or a vehicle and an obstacle) at any part on the front or rear side of vehicle. such collision should alert the driver of potential risk.

- **Service advertising**: service provider sends out messages to advertise services offered to an ITS-S such as Media downloading.

- **Vehicle and RSU data calibration**: RSU compares its sensor data or calculated traffic status to the data received from passing vehicles. It helps vehicles to detect if their sensors are broken down.

- **Remote diagnostic and just in time repair notification**: A road side unit having the capability to access to internet will enable any passing by vehicle to report about its current functional state to a local/remote diagnosis center and to receive just in time repair notification if having subscribed such service.

- **Automated overtake**: Fully-automated vehicles will need to perform overtake maneuver on two-way roads. Such maneuver may be dangerous as a quickly approaching vehicle may be out-of-range of vehicle sensors. Vehicles thus need to cooperate to allow a safe overtake without a risk of collision.

- **High density platooning**: is the creation of closely spaced multiple-vehicle chains on highway. Vehicles in the same platoon will exchange information in real-time to maintain a distance between them down to 1 meter. Vehicles thus need to constantly exchange kinematic state information to allow speeding up and braking while keeping the distance constant.

- **See through sensoring**: is the exchange of video information between a vehicle and the one behind it. For instance a vehicle behind a truck receives a video stream coming from the camera at the front of the truck. This will give the driver an extended vision of the environment thus allowing safer decision making (e.g. when the vehicle decides to overtake the truck). Such use case thus requires a high reliability, availability and data rate as well as a low latency.

- **High definition map download (HDMap)**: in fully autonomous driving, the use of usual 2D digital roadmaps is not sufficient. Indeed, autonomous vehicles require precise information about their complex environment. HDMap is a new generation of maps that could be used for this purpose. Such map have high precision at centimeter level accuracy but require high data rate to be downloaded by vehicles.

- **Traffic data collection** this use case has been introduced by SCOOP@F project. The vehicle sends information about position, speed, and direction to a back end service in order to better identify congested zones and react accordingly.

- **Accident zone warning** a driver detects that another vehicle (or himself) has been in an accident and signals it to the operator via his HMI. The operator broadcasts the information to road users, that could be in the relevance area of the road, in order to alert them of a potential danger.

4.3 Proposed use cases

If we look at the use cases previously described, we can see that only a few are security oriented. Most of them are application oriented. However, the security system has its own use cases to work properly. In this section, we propose five use cases related to security and privacy in C-ITS. Three of them are related to pseudonyms whereas two others are related to CTL/CRL and crypto-agility. Proposed use cases are described below:

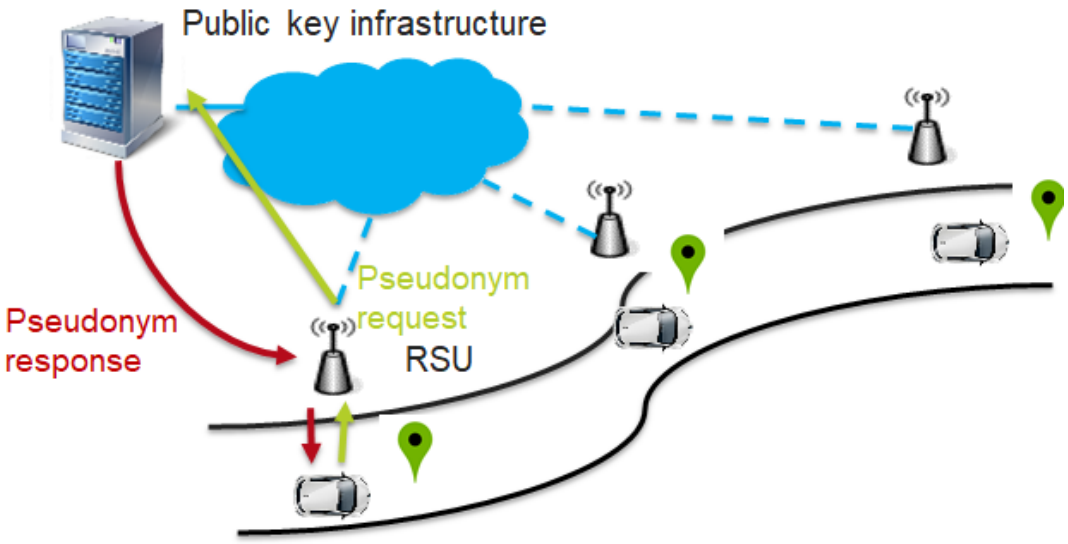

Figure 4.1: pseudonym reloading via a RSU providing access to Internet

- **Pseudonym reloading**: when a vehicle is low on pseudonym certificates it should be able to communicate with the PKI to request new certificates. This use case is all about informing vehicles about their possibility to access the PKI and how to handle it. For instance not all roadside units may provide an access to the Internet. Using cellular network or Wi-Fi hot-spots may also be a possibility for a vehicle to reach the PKI in the case of lack of roadside infrastructure. Figure 4.1 presents the use case. When the vehicle is in the range of an RSU, it sends a pseudonym request to the PKI. The PKI processes the request and sends back its response to the vehicle. In this use case, we consider that the vehicle uses ITS-G5, but in reality, this use case can be also done using ITS-G5 and cellular network.

- **Pseudonym change**: pseudonym change is the mechanism used to preserve drivers privacy. However, doing an efficient pseudonym change is not an easy task. Indeed if a vehicle is alone on the road and changes its pseudonym certificate, it is very easy to link the previous pseudonym with the new one, thus breaking all privacy. Moreover, frequent pseudonym changing may disturb safety applications [7] [8] which is in direct contradiction with the main objective of C-ITS (improving road safety). Therefore finding the best pseudonym change strategy is not easy task as many parameters are involved. This use case is presented in Figure 4.2. The vehicle in the figure has in its pool

two valid pseudonym certificates (Cert2, Cert3) and it is currently using Cert1 to sign the V2X messages. After a defined timer or number of kilometers, the vehicle changes its pseudonym certificate and uses Cert2. Many pseudonym change strategies exist in the literature, but none of them are standardized until now. In chapter 6 we study the feasibility of pseudonym linkage (tracking attack) using two pseudonym change strategies and two attacker model (mid-sized and global attacker).

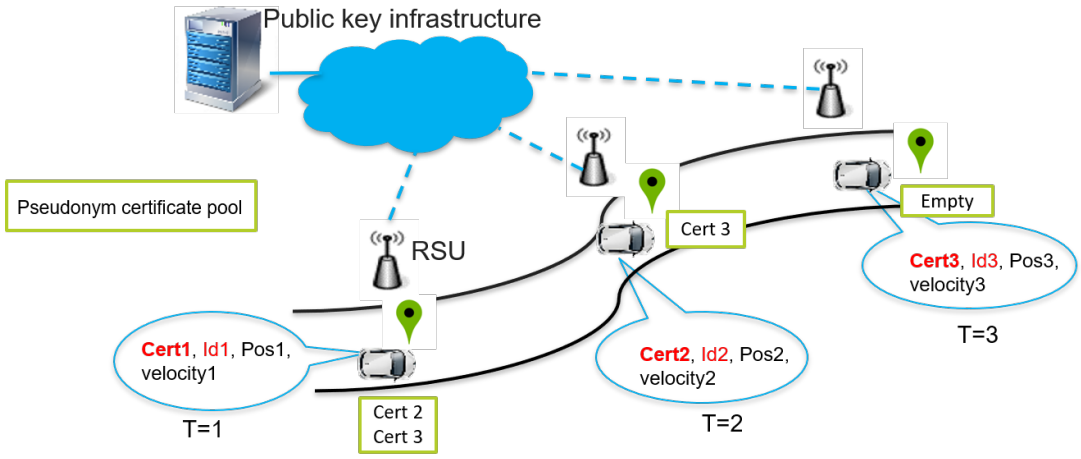

Figure 4.2: Pseudonym change use case

- **Lack of pseudonym**: it remains possible that a vehicle has no more pseudonym certificates left and no connectivity to the PKI is possible (e.g. because of the lack of network infrastructure) as presented in figure 4.3. In such scenario two modes are possible for the vehicle. The first one is the fail safe mode. The vehicle is not authorized anymore to send V2X messages as it cannot sign them. The vehicle thus should park in the best safe way by the side of the road. The second one is the fail operational mode. The vehicle has one backup pseudonym certificate with a higher validity period than the usual pseudonym certificates. It uses that certificate to continue sending V2X messages until it can reach again the PKI. However during this period of time it remains vulnerable to tracking attacks.

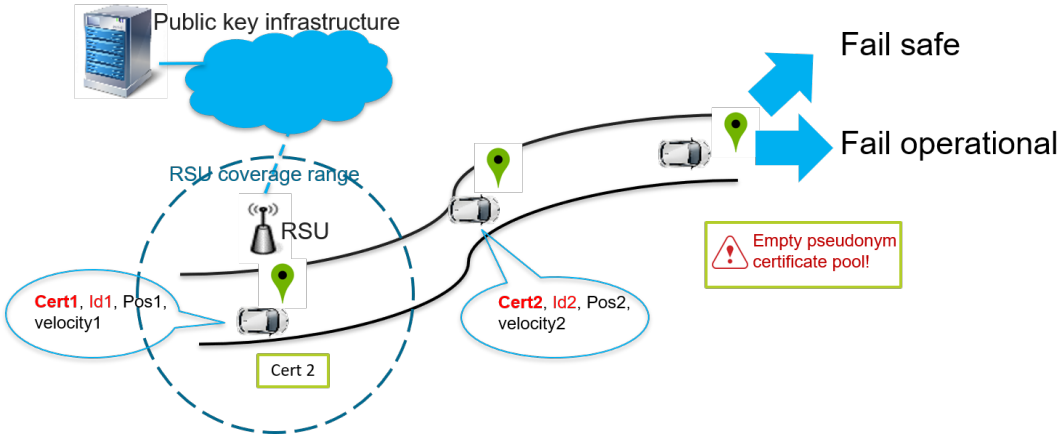

Figure 4.3: Lack of pseudonym use case

- **Distribution of Certificate Trust List (CTL) and Certificate Revocation List (CRL)**: CTL and CRL are lists that give information to the vehicles and roadside units about trusted and revoked PKI entities. Basically speaking, the CTL issued by a RCA contain the list of approved sub- CAs. CTL additionally contains DC URL access point. The CRL contains the list of PKI entities that have been revoked. Both lists thus enable vehicles and roadside units to be informed if a PKI entity has been compromised or not. This use case, presented in figure 4.4 focuses on the distribution of CTL and CRL to vehicles and roadside units.

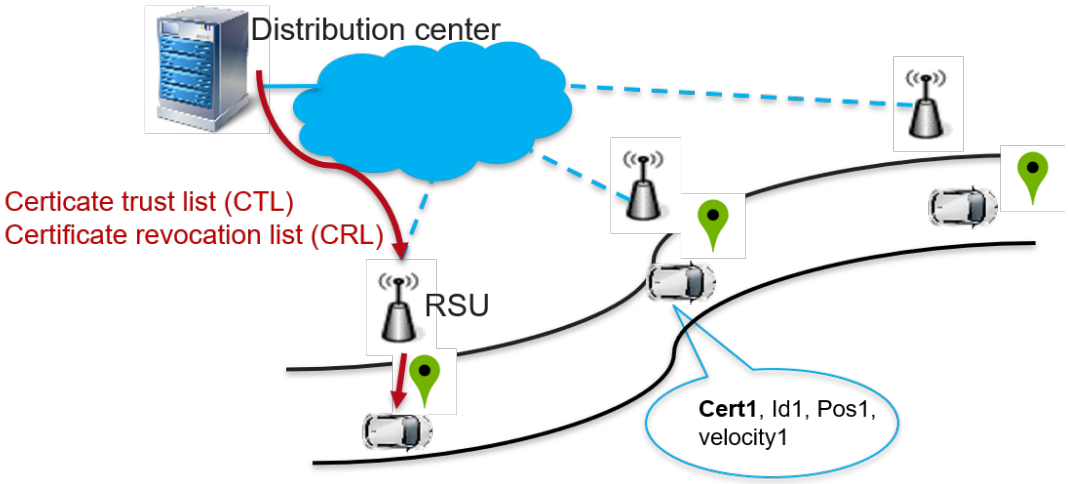

Figure 4.4: CRL/CTL reloading

- **Cryptographic Agility**: crypto-agility is the ability to migrate from a cryptographic algorithm to another one over the time. In the context of C-ITS the following two use cases are defined.

  - Capacity to support cryptographic algorithms: it is the capacity of the hardware to support cryptographic operations. For instance a change of the signature algorithm should still work without requiring hardware upgrade. Device should therefore implement a mechanism to communicate its capability of supporting such operations.
  - Verification of software authenticity and integrity: the equipment should not allow malicious software installation. To this end each software should be digitally signed in order to authorize installation of only trusted software.

4.4 Use case classification methodology

Due to the large number of use cases present in the literature, it is obvious that applying any process/method (e.g risk analysis) on them is a tough task. Therefore, there is a need to classify the use cases in clusters that share similar characteristics. Then the extraction of representative use cases from each cluster enables to get a subset of use cases to work with. In this section, we describe our proposed classification methodology.

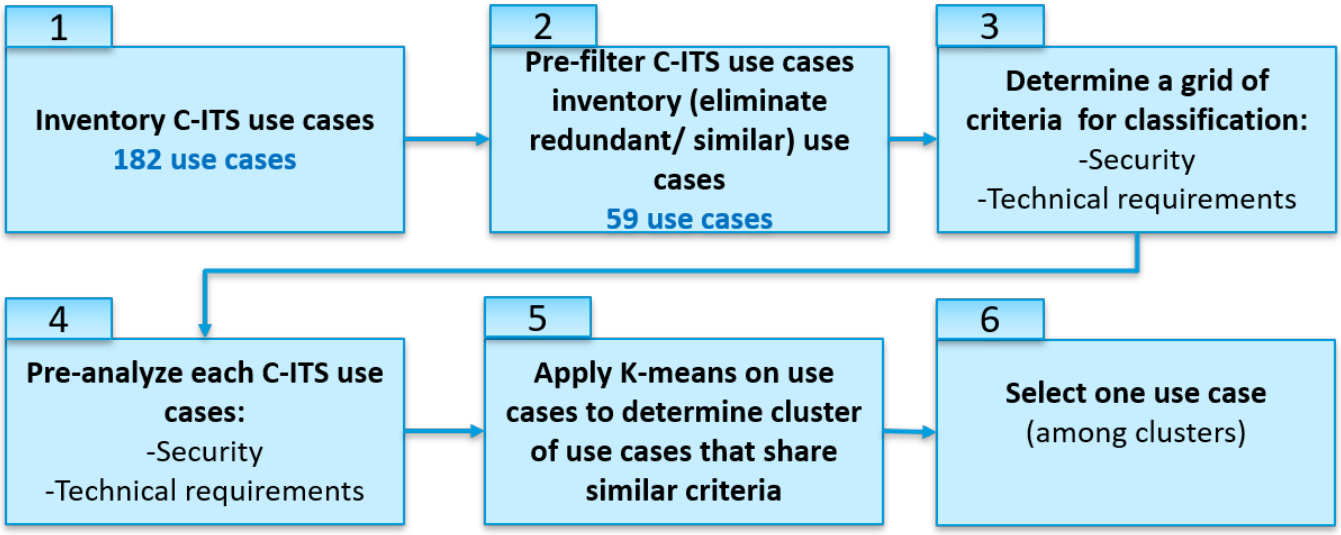

Figure 4.5: Classification methodology

4.4.1 Proposed classification methodology

The proposed classification methodology is depicted in figure 4.5. It consists of the following six steps.

1. We make an inventory of C-ITS use cases. We end up with a list of 182 use cases.

2. We pre-filter the list by removing redundant or similar use cases manually. We end up with the reduced list of 59 use cases presented in table 4.2 and 4.3.

3. In order to reduce even more this list, we classify use cases that share similar characteristics into clusters. To this end, we first define the classification criteria. Similar to [39], we focus on criteria related to security and technical requirements. The criteria we consider are presented in table 4.1 .

4. We then pre-analyze each use case by assigning them a corresponding value for each criteria. We end up with a 59x19 matrix (59 use cases with 19 criteria). We present this analysis for one use case. For example, the first use case in table 4.2, emergency vehicle approaching, the confidentiality is not important because it is a message that should be broadcasted to all the vehicles in the same area. Integrity is important because the drivers could react on the received message. Availability of this service is important because it permit the drivers to let the emergency vehicle pass. We note that we do not consider it very important because it is not safety critical, which means for connected vehicles driver is capable to see the emergency vehicle approaching and react by himself. Authenticity of the sending vehicle is very important because the vehicle should not accept any message without the proof of identity and the proof of vehicle type (emergency vehicle) of the sending vehicle. We do not consider that privacy is very important because the emergency vehicle is not the property of a specific person, gathered information about the vehicle's trajectory are worthless. Traceability is not important. Plausibility is very important to prevent disturbing info-traffic applications, juridical access is not important. We applied this analysis on all the use cases and we also studied the same use

cases based on technical requirements using the same logic. The detailed study is presented in table 4.3.

5. We apply the K-means algorithm on the matrix to classify the use cases into clusters. This step is splitted into two sub-steps: the first one is applying k-means on table 4.2, we aimed to classify UC based on security requirements and then the second step is applying K-means on table 4.3 to classify them based on technical requirements.

6. Finally, for each cluster we select a representative use case.

4.4.1.1 K-means clustering

K-means is a method of unsupervised learning used to automatically partition a data set into K clusters [40] [41]. Based on the study presented in [42], we believe that K-means is the best clustering algorithms that suits our needs. The first step consists of choosing the number of clusters *K*, and then the steps of the algorithm follows:

1. Place *K* points into the space represented by the objects that are being clustered. These points represent initial group centroids.

2. Assign each object to the group that has the closest centroid. The centroides are selected randomly, which means that if we repeat the algorithm multiple times, we can have different results. It all depends of the choice of the centroid at the beginning. However, in case of choosing the best clusters number *k*, if we repeat the algorithm multiple times, the results will be very similar.

3. When all objects are assigned, recalculate the positions of the *k* centroids.

4. Repeat steps 2 and 3 until the centroids no longer move. This generates a separation of the objects into groups from which the metric to be minimized can be calculated.

Security/Technical requirements	**Description**	***Possible values***
Authentication/ Authorization	Verification of the identity of a user or device.	*0:Irrelevant 1:Important 2:Very Important*
Confidentiality	Data access and disclosure for authorized users/devices only and privacy protection.	*0:Irrelevant 1:Important 2:Very Important*
Integrity	Ensuring that data have not been altered in an unauthorized manner.	*0:Irrelevant 1:Important 2:Very Important*
Traceability/ Auditability	Capability of keeping track of a given set or type of information to a given degree.	*0:Irrelevant 1:Important 2:Very Important*

Availability	Ensuring timely and reliable access to data.	*0:Irrelevant 1:Important 2:Very Important*
Anonymity/privacy	Use of a resource or service without disclosing the user's identity.	*0:Irrelevant 1:Important 2:Very Important*
Plausibility	Evaluation of data included in a message. Are they correct and realistic?	*0:Irrelevant 1:Important 2:Very Important*
Juridictional Access	Ability to a legal authority to access to the system data in case of dispute.	*0:Irrelevant 1:Important 2:Very Important*
Type of use case	-	*0:Road Safety 1:Traffic Efficiency 2:Other*
Driver's involvement	-	*0:Irrelevant 1:Awarness 2:Attention 3:Reaction 4:No involvement*
V2V communication	-	*0:No 1:Yes*
V2I communication	-	*0:No 1:Yes*
I2V communication	-	*0:No 1:Yes*
Use of cellular network	-	*0:Irrelevant link 1:Primary link 2:secondary*
Type of routing	-	*0:Broadcast 1:Multicast 2:Unicast*
Communication range	-	*0:Multi-hop 1:Single-hop*
Latency	-	*0:Highly critical (<300ms) 1:Citical (<5s) 2:Not critical (≥5s)*
Frequency of information sending	-	*0:High 1:Medium 2:Low*
Volume of exchanged data	-	*0:High 1:Medium 2:Low*
Quality of information	-	*0:Not critical 1:Critical 2:Very critical*

Table 4.1: Classification criteria

Source	**Use case**	Confidentiality	Integrity	Availability	Authenticity	Privacy	Traceability	Plausibility	Juridical access
ETSI	Emergency vehicle approaching	0	1	1	2	1	0	2	0
	Slow vehicle indication	0	1	1	1	1	1	2	1
	Across traffic turn collision risk warning	0	2	1	2	1	1	2	1
	Merging traffic turn collision risk warning	0	2	1	2	1	1	2	1
	Co-operative merging assistance	0	2	1	2	1	1	2	1
	Intersection collision warning	0	2	1	2	1	1	2	1
	Co-operative forward collision warning	0	1	1	2	1	1	2	1
	Lane change maneuver	0	2	1	2	1	1	2	1
	Emergency electronic brake lights	0	2	1	2	1	1	2	2
	Wrong way driving warning	0	2	2	2	1	1	2	2
	Stationary vehicle	0	1	1	2	1	1	2	1
	Traffic condition warning	0	1	1	1	0	1	1	1
	Signal violation warning	0	1	1	2	1	2	1	2
	Roadwork warning	0	1	1	2	1	1	1	1
	Weather information	0	1	1	2	0	0	1	0
	Decentralized floating car data	0	1	1	1	0	1	1	1
	Vulnerable road user warning	0	1	1	1	1	1	2	1
	Pre-crash sensing warning	0	2	2	2	1	2	2	2
	Co-operative glare reduction	0	1	1	1	1	1	1	1
	Motorcycle approaching indication	0	1	1	2	1	1	1	1
	Safety function out of normal condition warning	0	1	1	1	1	1	2	1
	SOS service	2	2	2	2	0	2	2	2
	Car rental/sharing	2	1	1	2	1	1	0	2
	Overtaking vehicle warning	0	2	2	2	1	1	2	1
	Co-operative adaptative cruise control	0	2	2	2	2	1	2	1
	Eco cooperative adaptative cruise control	0	2	2	2	2	1	2	1
	Traffic light optimal speed advisory	0	1	1	2	0	1	2	2
	Traffic information and recommended itinerary	0	2	0	2	0	1	2	1

	Public transport information	0	1	1	2	0	1	1	1
	In-vehicle signage	0	1	1	2	0	0	2	1
	Electronic toll collect	2	2	2	2	0	2	2	2
	Point of interest notification	0	1	1	1	0	1	2	1
	Stolen vehicle alert	2	2	1	2	0	2	2	2
	Fleet management	0	1	1	2	0	1	1	1
	Highway automation system	0	2	2	2	2	2	2	2
	Regulatory/contextual speed limits notification	0	1	1	2	0	1	2	1
	Map download and update	0	1	0	0	0	0	1	0
	Data provisioning	2	2	2	2	2	1	1	2
	Cooperative perception	0	2	1	2	2	1	2	1
	Longitudinal collision risk warning	0	1	1	2	1	0	2	1
	Service advertising	0	1	1	1	0	1	0	1
	Vehicle and RSU data calibration	1	2	1	2	1	2	0	1
US	OBE pseudonym certificate provisioning	2	2	2	2	2	1	2	2
	OBE pseudonym identification certificate provisioning	2	2	2	2	2	1	2	2
	RSE application certificate provisioning	2	2	2	2	2	1	2	2
	Misbehavior reporting	2	2	1	2	1	1	2	2
Cellular	Automated overtake	0	2	1	1	1	1	2	1
	High density platooning	0	2	2	2	2	1	2	1
	See through sensoring	0	1	1	1	1	1	2	1
	High definition map download (HDMap)	0	1	0	0	0	0	1	0
EU projects	Accident zone warning	0	1	1	1	1	1	2	1
	Human problem	2	1	1	2	2	1	1	0
	Remote diagnostic and just in time repair notification	2	2	1	2	1	2	2	2
	Collection of event data (by human driver)	1	2	2	2	1	2	1	1
Proposed use cases	Lack of pseudonyms	2	2	2	2	2	2	2	2
	Cryptoagility and software update	2	2	1	2	1	1	1	1
	Pseudonym reloading	2	2	2	2	2	2	2	2
	Distribution of certificate revocation and trust lists	0	2	2	2	0	1	1	1

	Pseudonym change	2	1	1	1	2	1	0	0		

Table 4.2: Use cases security and privacy requirements

Source	Use case	Driver's involvement	V2V communication	V2I communication	I2V communication	Use of cellular network	Type of routing	Communication range	Latency	Frequency of information sending	Volume of exchanged data	Quality of information
ETSI	Emergency vehicle approaching	2	1	1	1	2	0	1	0	0	1	0
	Slow vehicle indication	1	1	0	0	0	0	1	0	1	1	0
	Across traffic turn collision risk warning	1	1	0	0	0	0	0	1	0	1	1
	Merging traffic turn collision risk warning	1	1	0	0	0	0	0	1	0	1	1
	Co-operative merging assistance	1	1	0	0	0	0	0	1	0	1	1
	Intersection collision warning	2	1	1	1	0	0	1	0	0	1	2
	Co-operative forward collision warning	2	1	0	0	0	2	0	0	0	1	2
	Lane change manoeuvre	2	1	0	0	0	0	1	0	0	1	1
	Emergency electronic brake lights	2	1	0	0	0	0	0	0	2	1	2
	Wrong way driving warning	1	1	1	1	0	0	1	0	2	1	1
	Stationary vehicle	1	1	1	1	0	0	0	2	2	1	0
	Traffic condition warning	0	1	1	1	2	0	0	2	2	2	0
	Signal violation warning	1	0	0	1	0	0	0	1	1	1	1
	Roadwork warning	1	0	0	1	0	0	0	0	2	1	0
	Weather information	0	0	1	1	0	0	1	2	2	1	0
	Decentralized floating car data	1	1	1	1	0	0	0	1	1	1	1
	Vulnerable road user warning	1	1	1	1	0	0	0	0	0	2	1
	Pre-crash sensing warning	2	1	0	0	0	0	1	0	2	1	2
	Co-operative glare reduction	2	1	1	1	0	0	1	0	1	2	0

	Motorcycle approaching indication	1	1	1	1	0	0	0	0	1	1	1
	Safety function out of normal condition warning	1	1	1	1	0	0	0	0	1	1	1
	SOS service	2	0	1	1	2	2	1	0	1	1	2
	Car rental/sharing	0	0	1	1	2	2	1	1	0	0	0
	Overtaking vehicle warning	1	1	0	0	0	0	1	0	1	1	2
	Co-operative adaptative cruise control	3	1	0	0	0	1	1	0	0	0	2
	Eco cooperative adaptative cruise control	3	1	0	0	0	1	1	0	0	0	2
	Traffic light optimal speed advisory	2	0	0	1	0	0	0	0	1	1	0
	Traffic information and recommended itinerary	1	0	0	1	2	0	0	1	1	1	0
	Public transport information	0	0	0	1	2	0	0	1	2	1	0
	In-vehicle signage	2	0	0	1	0	0	1	0	1	1	2
	Electronic toll collect	0	0	1	1	1	2	1	0	0	1	1
	Point of interest notification	0	0	1	1	2	0	0	2	1	1	0
ETSI	Stolen vehicle alert	3	1	1	1	2	0	0	0	0	1	1
	Fleet management	0	0	1	1	1	0	0	2	1	1	0
	Highway automation system	3	1	0	0	0	1	0	0	0	0	2
	Regulatory/contextual speed limits notification	2	0	0	1	0	0	0	1	1	1	0
	Map download and update	3	0	1	1	2	1	0	0	0	1	1
	Data provisioning	3	0	1	1	1	2	1	0	0	0	2
	Cooperative perception	3	1	1	1	2	0	0	0	1	1	1
	Longitudinal collision risk warning	2	1	0	0	0	0	0	0	0	1	2
	Service advertising	0	0	0	1	2	0	0	1	1	1	0
	Vehicle and RSU data calibration	3	0	1	1	0	2	1	0	1	0	1
	OBE pseudonym certificate provisioning	3	0	1	1	2	2	1	0	0	0	2
	OBE pseudonym identification certificate provisioning	3	0	1	1	2	2	1	0	0	0	2
US	RSE application certificate provisioning	3	0	1	1	2	2	1	0	0	0	2
	Misbehavior reporting	3	0	1	1	2	2	1	0	0	0	2
	Automated overtake	3	1	1	1	1	1	0	0	0	0	2
Cellular	High density platooning	3	1	1	1	1	1	0	0	0	0	2

	See through sensoring	3	1	1	1	1	1	0	0	0	0	1
	High definition map download (HDMap)	3	0	1	1	1	2	1	0	0	0	2
EU projects	Accident zone warning	1	1	1	1	2	0	0	0	1	1	1
	Human problem	0	1	1	1	2	0	0	0	0	1	2
	Remote diagnostic and just in time repair notification	2	0	1	1	1	2	1	0	0	0	2
	Collection of event data (by human driver)	3	0	1	1	1	1	1	1	0	0	1
Proposed use cases	Lack of pseudonyms	3	0	1	1	2	2	0	0	0	0	2
	Crypto-agility and software update	3	0	1	1	1	2	1	0	0	0	2
	Pseudonym reloading	3	0	1	1	2	2	1	0	0	0	2
	Distribution of certificate revocation trust lists	3	0	1	1	2	2	1	0	1	0	2
	Pseudonym change	3	0	0	0	0	0	2	2	2	2	0

Table 4.3: Use cases technical requirements

4.4.2 Results

4.4.2.1 Silhouette

Silhouette refers to a method of interpretation and validation of clustering. The technique provides a succinct graphical representation of how well each object lies within the same cluster. Silhouette can apply on the data clustered via k-means. For each datum *i*, let *Ai* be the average dissimilarity of *i* with all other data within the same cluster. Many measures of dissimilarity can be used, in this work, we used the euclidean distance measure to calculate the dissimilarity. *Ai* represents how well *i* is assigned to its cluster (the smaller the value, the better the assignment). The average dissimilarity of point *i* to a cluster *C* is the average of the distance from *i* to points in *C*.

Let *Bi* be the lowest average dissimilarity of *i* to any other cluster, of which *i* is not a member. The cluster with this lowest average dissimilarity is said to be the ”neighbouring cluster” of *i* because it is the next best fit cluster for datum *i*. Silhouette is defined based on *Ai* and *Bi* in the equation 4.1:

$$S(i) = \frac{Bi - Ai}{max\{Ai, Bi\}} \tag{4.1}$$

S(i) is close to 1 when $Ai << Bi$. As *Ai* is a measure of how dissimilar *i* is to its own cluster, a small value means that it is well matched. Furthermore, a large *Bi* implies that *i* is badly matched to its neighboring cluster. Thus, *S(i)* = 1 means that the datum is perfectly clustered. If *S(i)* is negative then *i* is closer to the neighboring cluster. An *S(i)* near zero means that *i* is on the border of two clusters.

In this work, we tested the average silhouette value of all the clusters, when k = 2 to k = 10. We found that K= 5 is the best partitioning of our data. Figure 4.6 presents the silhouette of 5 use case's clusters based on security requirements and Figure 4.7 presents the silhouette of 5 use case's clusters based on technical requirements.

4.4.2.2 Principal Component Analysis (PCA)

The obtained result of the K-means algorithm is a vector of 19 dimensions (the number of criteria presented in table 4.1). As it is not possible to visualize a graph with 19 dimensions, we use the Principal Component Analysis (PCA) method to reduce the dimensions to two. PCA is a statistical procedure that is used to extract the essential part of the data in order to minimize the dimensionality of the data. Each point with n dimensions (n ¿ 2) has three or more multiple principal component (PC). In general, PC1 and PC2 represents 80% of the data. Figure 4.8 depicts the PCA of two-dimensions clustering based on security requirements, Figure 4.9 depicts the PCA of two-dimensions clustering based on technical requirements.

Results with K = 5. Each point on the graph is a use case and the color shows the cluster to which it belongs to. It also presents how close each cluster to all security requirements presented below. For example, for cluster C2 authenticity, traceability, plausibility and privacy are more important than other security requirements. For cluster C3, plausibility and traceability are less important than all other security requirements.

Table 4.4 presents the main criteria (security and technical) for each cluster. The main criteria is the criteria that is common to most of the use cases of the same cluster. One use case is selected from each cluster, as presented in table 4.4.

Cluster	**Main security criteria**	**Main technical criteria**	**Selected use case**
C1	Authenticity	Cellular network	CRL/CTL distribution
C2	Plausibility	Critical information	High density platooning
C3	Security and privacy	No driver involvement	Pseudonym reloading
C4	Integrity	Broadcast services	HD Map
C5	High authenticity, confidentiality	-	Pseudonym change

Table 4.4: Clustering results and main selected use case

4.5 Conclusion

In this chapter, our contribution is firstly the inventory of existing C-ITS use cases. We then extends this list by proposing new use cases that are mostly related to security and privacy aspects. In a second phase we propose a classification methodology that aims at extracting a subset of relevant use cases from the original list of use cases. To this end, we define security and technical criteria and apply the K-means algorithm. The obtained result is a classification of the use cases based on security criteria and a classification of the use cases based on technical criteria. Use cases in a same cluster share similar criteria. We then select one representative use case for each cluster, ending up with a final list of 5 use cases. In the next chapter, we will apply the Threat Vulnerability Risk Assessment (TVRA) method on

three use cases (among the selected use cases). the two use cases (high density platooning, HD Map) may be studied later in another thesis.

Figure 4.6: Silhouette score for use cases clustering based on security and privacy criteria

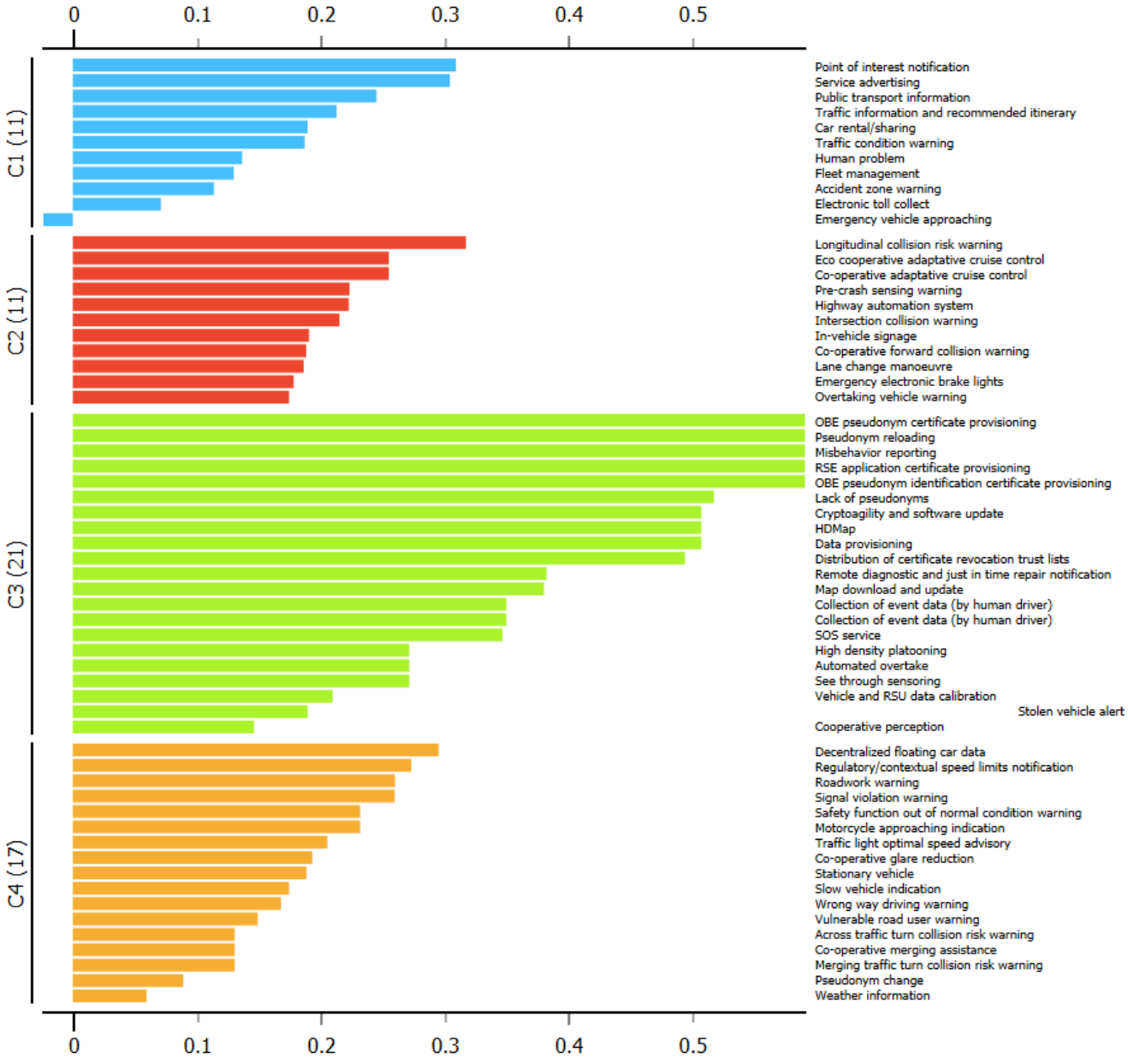

Figure 4.7: Silhouette score for use cases clustering based on technical criteria

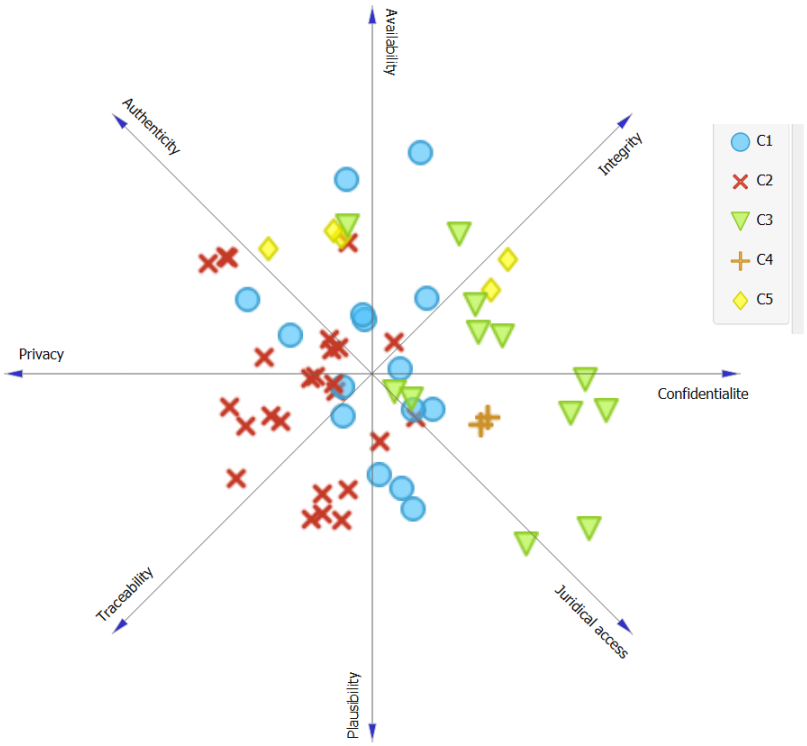

Figure 4.8: Principal Component Analysis (PCA) for use cases – Security and privacy criteria classification

Figure 4.9: Principal Component Analysis (PCA) for use cases – technical criteria classification

Chapter 5

Risk analysis

A risk assessment is used to identify and analyze potential threats and vulnerabilities. The risk assessment is important to understand and measure the level of the risk involved and hence, decide on the appropriate measures and controls to manage them.

5.1 Related works

Many risk assessment methods exist in the literature such as Expression des Besoins et Identification des Objectifs de Securite (EBIOS), Threat Vulnerability Risk Assessment (TVRA), etc

Berrehili et al. [43] applies the EBIOS method in the internet of things (IoT) domain. The motivation of their work is to determine the highest security risks on the IoT applications. This help the developers build applications in a secure way.

The Threat Vulnerability and Risk Analysis (TVRA) method is proposed first by the ETSI [38]. It is used to identify risks of the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security countermeasures that will minimize that risk [44] . The importance of the TVRA method is that it is designed by ETSI for any fixed and mobile communication and internetworking systems IoT,... and has been applied to ITS.

The difference between EBIOS and TVRA is that EBIOS is a generic method However TVRA is a detailed method and is usually used to determine specific vulnerabilities. For example, using EBIOS, we find a vulnerable interface that should be protected, otherwise using TVRA we should go more in the details (a vulnerable interface permits an attacker do buffer overflow). This is because in EBIOS, we define only the context of the system without going deep into the assets details. Obviously, the difference will impact the countermeasure, using EBIOS we will propose to use a firewall to protect the vulnerable interface. on the other hand, using TVRA, we will propose to resolve the problem of the buffer overflow.

Moalla el al. [45] applied the TVRA method on ITS communication architecture. The result of their work is an analysis on the impact of threats related to wireless communications and threats specific to the ITS.

In this thesis, our second contribution consists of applying TVRA method on selected use cases issued from our first contribution presented in chapter 4.

5.2 Threat vulnerability risk analysis (TVRA)

5.2.1 TVRA method description

In our analysis, we use the TVRA method. It consists of the steps presented in figure 5.1 and described below [38] .

1. Identification of the Target of Evaluation (TOE): the first step of TVRA is to have a clear definition of the scope, purpose and goal of the analysis. A comprehensive description of the Target Of Evaluation (TOE) and its environment should be produced.

2. Identification of the objectives: the description of the security aims and issues to be resolved should be listed.

3. Assets: inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2. In C-ITS, assets can be physical, logical, functional and human. Physical assets are the equipment that we want to protect, logical assets are the information stored in and handled by the physical assets and functional asset are the functions or the modules that should be protected.

4. Threats: identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

5. Impact: quantifying the impact of the threats. It is composed of two steps, first calculate the value of attack potential. It is the sum of the values mapped with factors presented in table 10.3 (see Annex 1) Time + Expertise + Knowledge + Opportunity + Equipment. Second, attack potential values are mapped with attack potential required to exploit attack as presented in table 10.4.

6. Likelihood: quantifying the occurrence likelihood. It consists of mapping the vulnerability rating with the threat level to identify the likelihood of the attack as presented in table 10.2.

7. Risk: first, the overall impact, shown in table 10.6, is determined by summing the asset impact value from table 10.1 and the attack intensity value from table 10.7. Then, the risk is established using equation 5.1. The value is then mapped using table 10.5.

8. Countermeasure: identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

$$Risk = likelihood * impact \tag{5.1}$$

5.2.2 Application of TVRA on selected use cases

1. **Target of evaluation**: in our analysis, we apply the TVRA on use cases that we selected in chapter 2. We choose three use cases that are related to security and privacy from our first contribution.

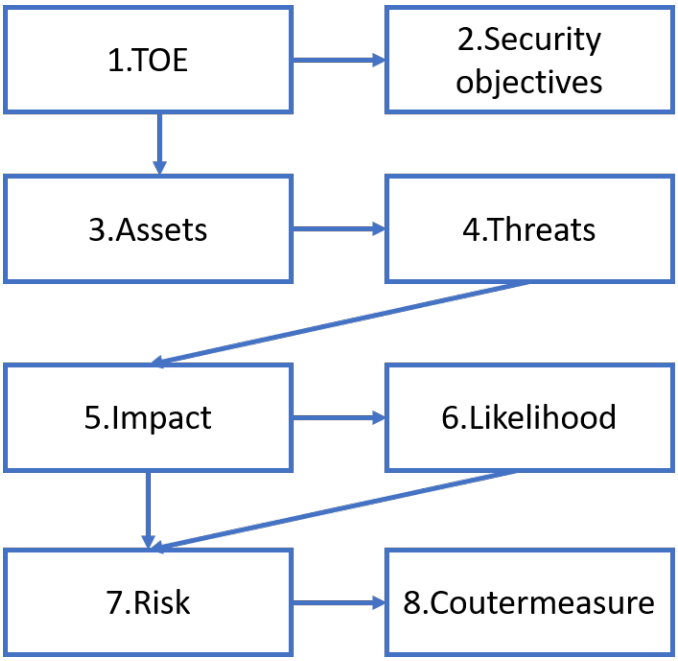

Figure 5.1: TVRA

The use cases are pseudonym change, pseudonym reloading and CRL/CTL distribution. Thus, our Target of Evaluation (TOE) is an interoperable vehicle that can use the three use cases listed above.

Figure 5.2 presents the TOE considered in our analysis. Cameras, radars, and lidars and other sensors are not part of our TOE.

2. **Security objectives**: the security objectives that need to be guaranteed in the three selected use cases are:

   - Availability: Some services are crucial such as PKI services. Vehicles need pseudonym certificates to sign their messages, certificates generation services on PKI are paramount. As well as, CRL/CTL distribution service keeps the vehicle up to date in the list of revoked and trusted entities.
   - Authentication: PKI shall authenticate any vehicle requesting a pseudonym certificate.
   - Integrity: messages sent by a vehicle shall not be modified in order to be treated by the PKI in case of pseudonym reloading. Messages shall not be modified in order to be considered by other vehicles. CRL/CTL lists shall not be modified.
   - Confidentiality: requests sent to the PKI shall be protected, only the PKI have the right to treat the request. Messages exchanged between vehicles do not require confidentiality, since the objective of the V2V messages is to broadcast kinematic information to be analyzed by other vehicles.
   - Privacy: during pseudonym reloading process, vehicle's privacy towards the operator should be guaranteed.

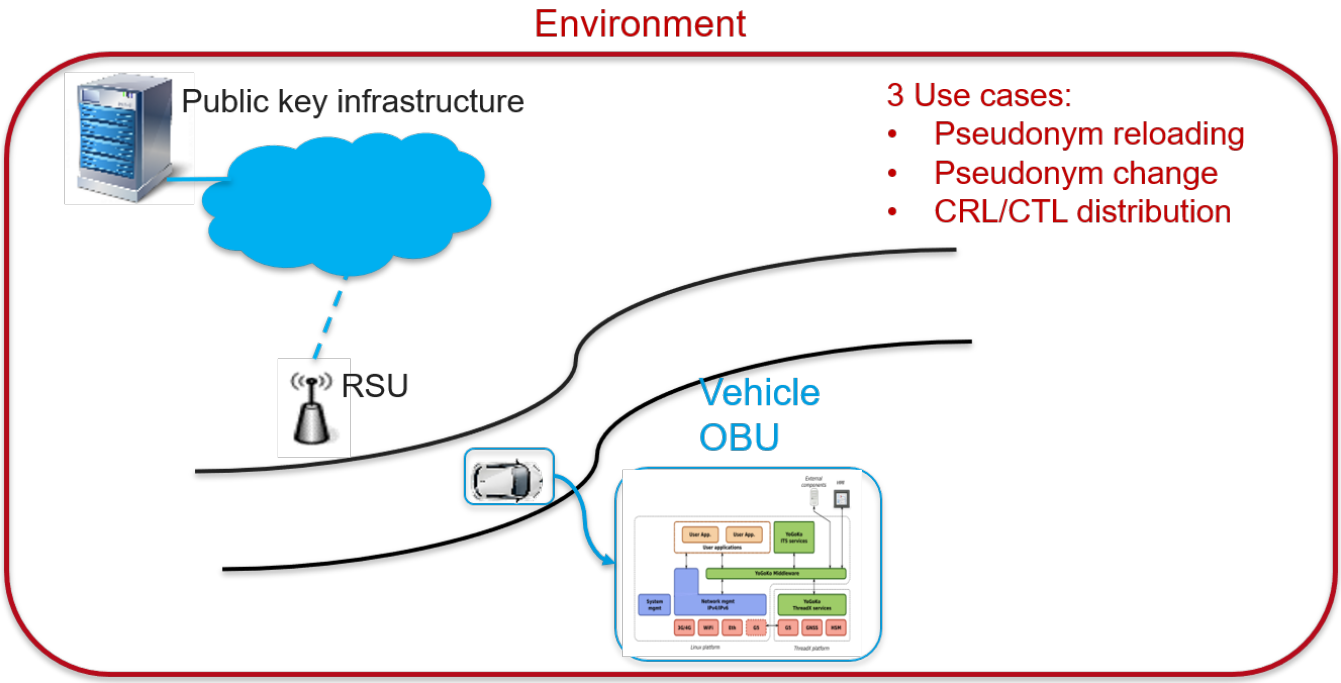

Figure 5.2: Target of evaluation

3. **Assets**: physical asset is an On Board Unit (OBU) that implement V2X communication and V2X security stack. Logical assets considered in our analysis are listed below:

   - Pseudonym certificate: it is a pseudonym identity used by the vehicle for communication. It prevents attacker to link the exchanged messages by changing the identity depending on a pseudonym change strategy. Each vehicle has a pool of valid and certified pseudonyms that could be used during the vehicle's trajectory.
   - Enrollment certificate: it is the long-term identity that is not used during the communication. It is used by the vehicle only for requesting a new pseudonym certificate from the Authorization Authority (AA).
   - Root certificate: it is the certificate of the Root authority.
   - EA/AA certificates: the certificate of the enrollment authority and the certificate of the authorization authority should be protected to prevent any manipulation.
   - Certificate Revocation List (CRL) and Certificate Trust List (CTL): CRL is issued and signed by the RCA verification key. It contains the CA certificates identifiers that are no longer worthy of being trusted. CTL contains the valid access point for security services.
   - Cryptographic keys: the keys that are used for encryption and decryption.
   - ITS Messages: exchanged messages such as Cooperative awareness message (CAM) and Decentralized Environmental Notification Message (DENM).

   Functional asset is pseudonym change strategies that define when to change pseudonym certificate by the vehicle. In our analysis, we do not consider human assets. In TVRA, asset impact should be

quantified using table 10.1. Values can be low impact, medium impact and high impact. It depends on how harmful the attack is on the assets.

4. **Identification of vulnerabilities and threat level**: the list of vulnerabilities are presented in table 5.1 and described below:

   - Sybil attack: Sybil attack was proposed first by Douceur [46]. A vehicle possesses usually multiple pseudonym certificates at the same time called also pool of pseudonyms. The sybil attack consists of using one or more valid pseudonyms by a vehicle at the same time. The threat agent can be a vehicle with valid keying material. An example of this attack could be an attacker who wants to enjoy the road alone or empty the street next to his house. To this end, he creates a sybil attack to simulate a congestion in an area, in order to cheat the info-traffic applications, so that they redirect traffic to other roads.
   - Location tracking attack: it consists of collecting all the exchanged messages in a specified area or multiple area, and analyzing their contents to identify which messages are sent by the same vehicle. This enables the attacker to track the vehicle and build drivers profiles for vehicles. The threat agent can be an eavesdropper with programmable radio receivers to receive exchanged CAM messages in a specific area.
   - Alteration of trust anchor information: modification of the RCA certificate or/and the EA/AA certificate could impact all communication information sent or received by the vehicle.
   - False message injection: there is no mechanism to detect that the received Cooperative Awareness Message (CAM)is plausible or not (position plausibility, etc)

   All the attacks listed above already exist in the literature. In this thesis we found three vulnerabilities that we propose for analysis:

   - Pseudonym change strategy inhibition: changing the pseudonym is triggered by a pseudonym change strategy implemented in the vehicle. If a vehicle does not change its pseudonym identity for a while, it will be traceable and thus impact the privacy of the users. An attacker can block the pseudonym change.
   - Exhaust of the pseudonym pool: when a vehicle sends a CAM, it is possible for an eavesdropper to send a CAM with the same ID. The originating vehicle receives this message and believes that another vehicle is using the same ID and thus, it changes directly its pseudonym. The repetition of this act may exhaust the pseudonym pool of the targeted vehicle.
   - CRL/CTL substitution: certificate revocation list and certificate trust list are paramount and any modification or substitution of these lists can impact trust on the whole system.

   The following factors shall be evaluated during analysis to determine the weight of the attack potential required to exploit a vulnerability. Time, expertise, system knowledge, opportunity, and equipment.

5. **Establishment of the risks**: the results of this analysis is the risk of each attack. All the steps and details are presented in table 5.1. We present the risk establishment of Sybil attack:

- Time: we consider that 5 months are enough to perform Sybil attack.
- Expertise: we consider that the attack should have good expertise in the system.
- Knowledge: to perform Sybil attack, attacker should know the message format used, frequency of sending messages etc.. such information are public and can be found in documents published by standards or white papers on the internet.
- Opportunity: we consider that an unlimited access is needed by the attacker to perform his attack. If he will use its vehicle to create Sybil attack. He need to access the existing pseudonym pool for all the attack duration.
- Equipment: attacker needs a specialized equipment to perform Sybil attack. Creating messages can be done using any simple unit, but sending a very large number of messages need a specialized equipment in order to perform the attack well.
- Threat level: Sybil attack is critical for C-ITS, because it has impact on information plausibility and thus impacts user's safety.
- Asset impact: the impact of Sybil on assets is high.
- intensity: Sybil attack can be performed in multiple instances on the same vehicle or even on multiple vehicles, it depends on the attacker's capabilities.

Threat	Attack	Range	Value	Potential	Likelihood	Impact	Risk
Sybil attack	Time	$\leq 5months$	15	25 (Beyond high)	2 (Possible)	3	6 (Critical)
	Expertise	Expert	6				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	Heavy level of multiple instances	2				
Location tracking attack	Time	$\leq 6months$	17	27 (Beyond high)	2 (Possible)	3	6 (Critical)
	Expertise	Expert	6				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	heavy level of multiple instances	2				
False message injection	Time	$\leq 1day$	0	7 (Basic)	3 (Very likely)	2	6 (Critical)
	Expertise	Proficient	3				
	Knowledge	Public	0				
	Opportunity	unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	medium	2				
	Intensity	single instance of attack	0				
Alteration of trust anchor	Time	$> 6months$	19				
	Expertise	Multiple experts	8				

information	Knowledge	Critical	11	57 (Beyond high)	3 (Possible)	3	9 (Critical)
	Opportunity	Difficult	10				
	Equipment	Multiple bespoke	9				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	single instance of attack	0				
Pseudonym change strategy inhibition	Time	≤ 5 months	15	42 (Beyond high)	1 (Very unlikely)	2	2 (Minor)
	Expertise	Expert	6				
	Knowledge	sensitive	7				
	Opportunity	Difficult	10				
	Equipment	specialized	4				
	Threat level	moderate	-				
	Asset impact	medium	2				
	Intensity	single instance of attack	0				
Exhaust the pseudonym pool	Time	≤ 3 months	0	7 (Basic)	3 (Very likely)	3	9 (Critical)
	Expertise	proficient	3				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				
	Threat level	Critical	-				
	Asset impact	High	3				
	Intensity	moderate level of multiple instances	1				
CRL/CTL substitution	Time	≤ 3 months	0	7	3	3	9
	Expertise	proficient	3				
	Knowledge	public	0				
	Opportunity	Unlimited access	0				
	Equipment	specialized	4				

	Threat level	Critical	-	(Basic)	(Very likely)		(Critical)
	Asset impact	High	3				
	Intensity	moderate level of multiple instances	1				

Table 5.1: Risk establishment

6. **Countermeasures**: security countermeasures are assets that are added to the system to reduce the weighted risk to the system. In order to be protected against the Sybil attack, we propose some countermeasures: limit the number of valid pseudonyms at the same time could help to minimize the likelihood of occurrence. The implementation of misbehavior detection could help to detect sybil vehicles. Misbehavior detection can also be countermeasure for the exhaust of pseudonym pool attack. The countermeasure of the tracking attack is to use a robust pseudonym strategy. Our next step will be the study of the robustness of the pseudonym change proposed by the Car2car. The countermeasure for false message injection attack is Plausibility Checks(PC). PC are crucial and it can help to filter not plausible messages. Kamel et al. [47] proposed a list of checks that could be implemented in order to detect a misbehaving entity. In order to deal with alteration of trust anchor information and CRL/CTL substitution, we propose to do integrity checks on existing trust anchor information and CRL/CTL lists.

5.3 Conclusion

In this chapter, we identified prior C-ITS security issues. We conducted a risk analysis based on ETSI TVRA methodology. TVRA permits analysing the risks of vulnerabilities based on multiple criteria such as expertise, knowledge, opportunity of the attacker, equipment and time needed to perform the attack. We studied potential vulnerabilities that may apply on three use cases: pseudonym reloading, pseudonym change, and CRL distribution. We then proposed several countermeasures that could handle these attacks. In the next chapter, we will study and implement more deeply some of the proposed attacks: tracking attack, sybil attack, CRL substitution and exhaust of pseudonym pool attack.

Threat	Countermeasure
Sybil	Limit the number of valid pseudonyms Misbehavior detection
Location tracking	Use of robust pseudonym change strategy
False message injection	Plausibility checks
Alteration of trust anchor information	Integrity checks
Pseudonym change strategy inhibition	Fix maximum threshold to perform a pseudonym change
Exhaust of the pseudonym pool	Misbehavior detection
CRL/CTL substitution	Integrity checks

Chapter 6

Attacks

Risk analysis shows that many attacks are possible in C-ITS. In this chapter, we implement some critical attacks found in risk analysis. Our aim is to study if the attacks are feasible or not on real equipment, and if they are feasible, then how to deal with ?

For Sybil attack, we demonstrate the feasibility of Sybil attack on real equipment used in the SCA project. Then, we propose a detection platform to detect vehicle's performing Sybil attack. For the tracking attack, we implement two attacker models: the first one is global and the second is mid-sized. For CRL substitution and exhaust of pseudonym pool (EPP), we demonstrate the feasibility of these attacks on real equipment, and we propose a scheme to deal with them.

6.1 Sybil attack

6.1.1 Sybil attack description

The pseudonym certificates are used by vehicles to sign their V2X messages. Vehicles frequently change their pseudonyms to avoid tracking and protect their privacy. Each vehicle uses a single pseudonym certificate for a certain time period to sign its generated V2X message. To ensure the ability of vehicles to continuously send V2X messages without being traceable, it is necessary that several valid pseudonyms are simultaneously available. That's what we call a pseudonym pool. The European Commission recommends the use of a maximum pool of 100 valid pseudonym certificates [48]. When a vehicle has a low pool, it sends requests to the PKI to refill its pool with new pseudonym certificates. Notice that vehicles shall not use more than one pseudonym certificate during a certain period of time to sign their messages. However, a malicious vehicle may intentionally use multiple valid pseudonym certificates at the same time to create non existing vehicles (called ghosts), which results in a Sybil attack.

Depending on the attackers objective, the Sybil attack may take different forms. We propose a classification into 4 categories:

1. **Traffic Congestion Sybil (S1)**: as shown in figure 6.1, the attacker (blue vehicle) uses valid pseudonyms to simulate multiple ghost vehicles. Vehicles within the communication range of the malicious vehicle receive the fake messages and conclude that a congestion occurs on the road. The attacker intelligently calculates the kinematic data for the ghost vehicles such that the fake messages have

plausible and coherent contents (position on the road, velocity is coherent with maximum velocity on the road, etc).

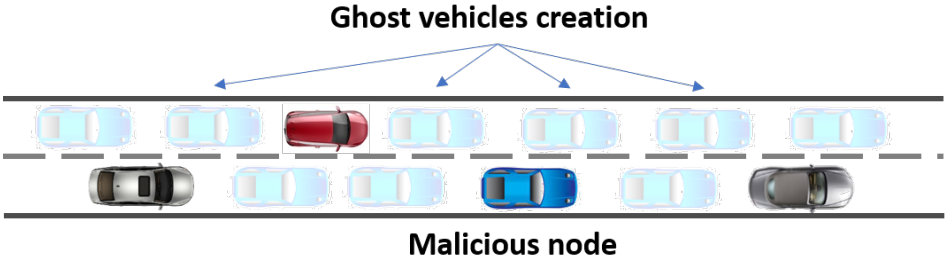

Figure 6.1: S1: Traffic congestion Sybil

2. **Data replay Sybil (S2)**: this attack consists of reporting a legitimate vehicle as malicious vehicle. The attacker chooses a victim vehicle and creates messages containing positions broadcasted by the victim vehicle. As shown in figure 6.2, the attacker (blue vehicle) sends at time t=1 a message containing the same position (X1) as the victim vehicle (red vehicle). The attacker continues by sending the same position of victim vehicle for a certain time.

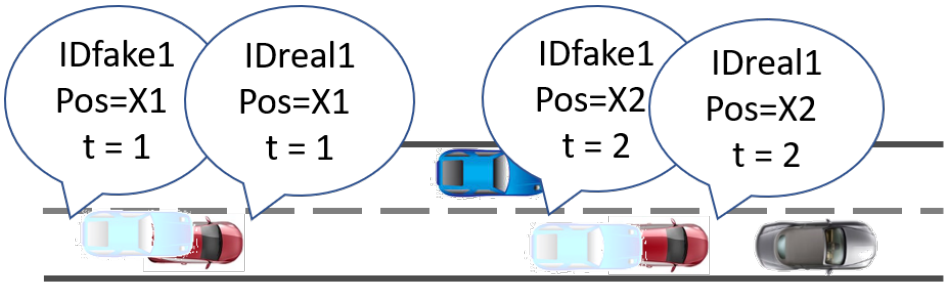

Figure 6.2: S2: Data replay Sybil

3. **Dos Random Sybil (S3)**: as shown in figure 6.3, the attacker creates messages with random data (e.g., the position is not on the road). The attacker (blue vehicle) uses a different pseudonym for every sent message. The motivation behind such attack could be to overwhelm the misbehavior detection algorithms of neighboring vehicles.

4. **Dos Disruptive Sybil (S4)**: this attack is a combination between S2 and S3. As shown in figure 6.4, the attacker uses a different pseudonym for each message but does not fill them with random data. Instead, the transmitted data is based on the ones received from the neighboring vehicles. The difference between S2 and S4 is that S4 does not follow one victim, the attacker is trying to disturb the system with sudden appearance of vehicles. For example, the attacker (blue vehicle) sends at time t=1 a message containing a position (pos=X1), and at time t=2 a message containing another position (pos=X2) which is the position of another vehicle. The motivation of the attacker could be the degradation of the safety system quality thus decreasing the reliability of the exchanged information.

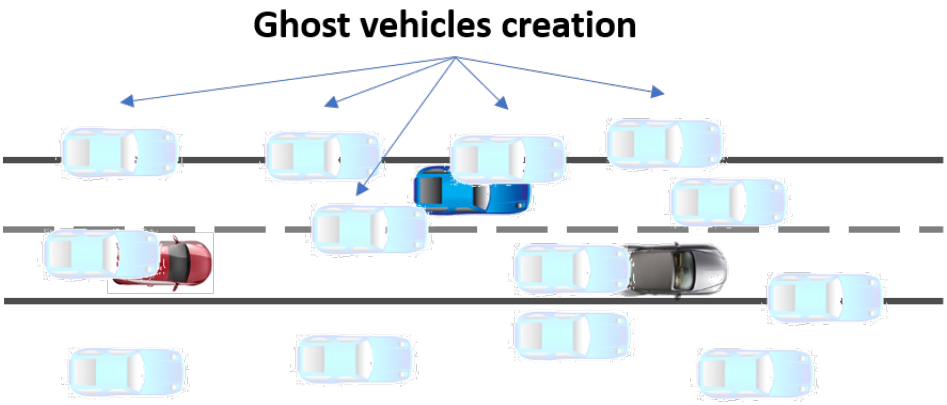

Figure 6.3: S3: Dos Random Sybil

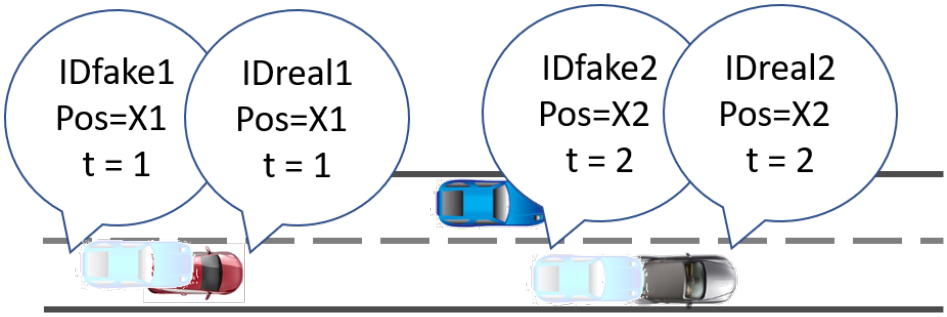

Figure 6.4: S4: Dos disruptive Sybil

6.1.2 Related works

Sybil attack was first introduced by Douceur in [46]. Due to the important damages it may cause in C-ITS systems, researchers have proposed several detection approaches.

Pouyan et al. [49] present three methods for local Sybil attack detection. The first method called resource testing method, assumes that a radio network entity cannot send and receive on the same channel at the same time. This detection method is not valid in vehicular networks because vehicles are authorized to send via multiple channels. The second method called position verification method assumes that a vehicle can be localized at only one position at the same time. The third method encryption and authentication based methods. It assumes that using a PKI is enough to detect Sybil attack. In our analysis, we consider that a legitimate entity with valid key materials can perform a Sybil attack, especially because the pseudonym certificates used in the Sybil attack are valid and are delivered by the PKI.

Hao et al. [50] propose a protocol that detects Sybil nodes in a cooperative way by examining the consistency between the vehicles positions and those of their neighbors. The idea is based on detecting the sudden appearance of a vehicle or of multiple vehicles as well as on evaluating the number of neighbors. When a vehicle detects locally that a neighbor is potentially malicious, it broadcasts a warning message to have the confirmation from other neighbors that an attack is occurring. When the number of vehicles that confirm that an attack is occurring is greater than a threshold, the identified vehicle may be quarantined for a certain period of time or reported to the MA. Cooperative detection systems are not reliable because the attacker takes part of the community and could distort the detection procedure. Moreover, it requires an honest majority to work properly.

Ghaleb et al. [51] propose a local misbehavior detection model based on artificial neural network. Some features are used to decide if a vehicle is misbehaving or not. In our opinion, local detection is insufficient as it is based on captured information by the vehicle only. A global system that has access to more misbehavior reports is required to improve the detection system.

Shrestha et. al [52] proposes a Sybil attack detection based on signal strength. The solution may work in case of uniform distribution of vehicles on the road. The problem of this solution is that it can not work in heavy traffic conditions when the distance between vehicles can be less than 10 m.

Gantsou et.al [53] propose a Sybil attack detection based on MAC address detection. The problem of this solution is that according to ETSI standard, the vehicle is supposed to change all their identities when they change their pseudonym (including the MAC address) in order to protect privacy. The usual behavior is changing the MAC address in case of pseudonym change; thus, this solution is not applicable for our system.

Sharma et.al [54] propose a detection method that consists of creating a list of neighbors based on received CAM (beacon) packets at each interval of time. The list is stored and broadcasted to vehicles in its range. Vehicles then calculate an evidence based on the idea that a Sybil vehicle has the same physical properties and same neighbor set. Vehicles using this detection method should broadcast the list of the vehicles behind and in front of it. This may load the communication channel.

The results of our risk analysis show that the Sybil attack is critical in C-ITS context. In fact, the severity of Sybil attack is that attacker can perform any other attack and change his pseudonym certificate to hide himself. Thus, we consider that a detection of Sybil attackers is paramount in C-ITS. Our analysis

Reference	Title	Detection method
Hao et al. [50]	Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs	local cooperative detection
Ghaleb et al. [51]	An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications	local non-cooperative detection
Shrestha et. al [52]	Sybil Attack Detection in Vehicular Network based on Received Signal Strength	local non-cooperative detection
Gantsou et.al [53]	On the Use of Security Analytics for Attack Detection In Vehicular Ad Hoc Networks	local non-cooperative detection
Sharma et.al [54]	Sybil Attack Prevention and Detection in Vehicular Ad hoc Network	local cooperative detection

Table 6.1: Sybil attack detection methods in the literature

of the existing works, presented also in table 6.1 show that most of the proposed solutions for Sybil attack detection in C-ITS focus on local (cooperative and non cooperative) detection. Local detection is not sufficient for the following reasons:

- **Local non cooperative detection is not sufficient**: local detection checks consist of performing some consistency and plausibility checks on received messages. Those checks can not be trusted all the time, because data in V2X messages may be altered due to sensors or cameras problem. For example, if a vehicle receives a message indicating a position that is too far from its current position, this means that either the vehicle's GPS is not working, or the vehicle is receiving a forged message from an attacker. A vehicle by itself can not differentiate data incoherence due to a faulty device or forged message by attacker. Thus, local detection may detect a malfunction as a misbehavior. Thus, local non cooperative is not sufficient.
- **Local cooperative detection is not sufficient**: in cooperative detection, the attacker is part of the environment, thus it can adapt its attack to deal with the detection checks on the victim's vehicle side. For example, if the cooperative detection is based on a voting mechanism, the attacker can easily change the result. If a vehicle detects a misbehaving entity, it sends the information to ask the neighboring vehicles if they vote that the detected vehicle is misbehaving or not. An attacker with valid pseudonyms can respond with multiple messages that the entity is not misbehaving, which will impact the result.

Global detection is therefore crucial and is still not studied well in the context of C-ITS. We propose to study the solution of a centralized entity (MA) that investigates and decides if the vehicle is misbehaving or not. In this thesis, our third contribution consists of two parts: the first one consists of proposing a test-bed to show the feasibility of the Sybil attack on real equipment, and the second part consists of the proposition of Sybil attack detection mechanism. The proposed mechanism consists of detecting Sybil

attack and identifying the Sybil attack type following the classification presented in section 6.1.1 (i.e is the attack of type S1, S2, S3, or S4).

6.1.3 Sybil attack feasibility on real equipment

Within the IRT SystemX SCA project, we have access to an on-board unit (OBU) from YoGoKo (YBOX-VEHI-1603). This on-board unit implements the communication and security stacks which are compliant with the ETSI standards and is reserved to be integrated inside the vehicle.

6.1.3.1 Attack implementation

For Sybil attack, we assume the following hypotheses:

- We have two vehicles represented by two different OBUs communicating over ITS-G5 and they are operable (i.e vehicles have an enrollment certificate and a pool of valid pseudonyms).
- One OBU is considered as the attacker's vehicle, and the other is the victim's vehicle.
- We are not using the HSM. Secret keys and pseudonym certificates are stored on the host CPU memory of the system.
- We dispose a trace of CAMs respecting the message format described in ETSI standards.

In order to represent attacks against our asset (vehicle OBU), we use the attack tree. It consists of trees with the final desired goal as the root node and different ways of achieving that goal as child nodes. Each child node of the root becomes a sub-goal, and children of that node are ways to achieve that sub-goal. If one of those nodes cannot be divided further, it is a leaf node. Otherwise, those nodes are treated as sub-goals separately and are divided continually until all the events become leaf nodes. According to the logical relationship among them, those nodes, which are linked with an "OR-gate" or "AND-gate", are OR nodes and AND nodes respectively. Figure 6.5 presents the general tree for Sybil attack. Pink cells represent the path we choose to perform Sybil attack on our work. As we can see from the tree, we followed three steps:

First step: We develop a malicious code (Sybil attack code). This code will generate different CAM messages with different pseudonyms. Simultaneously, this will be done over three steps.

1. We must have a starting point which is a valid CAM message (well-formed CAM that respects the ETSI standard message format). We can get a CAM message either by sniffing broadcasted CAMs or by using a saved or memorized a CAM message.
2. We need to modify some fields in the CAM message taken as an input. Some fields should change when pseudonym change is triggered. All ITS-S IDs are changed at the same time, such as the stationID, GeoNetworking source address and MAC source address. In addition, the generationDeltaTime corresponds to the time reference position in the CAM, considered as time of the CAM generation. We need to update it according to ETSI EN 302 637-2 [11].

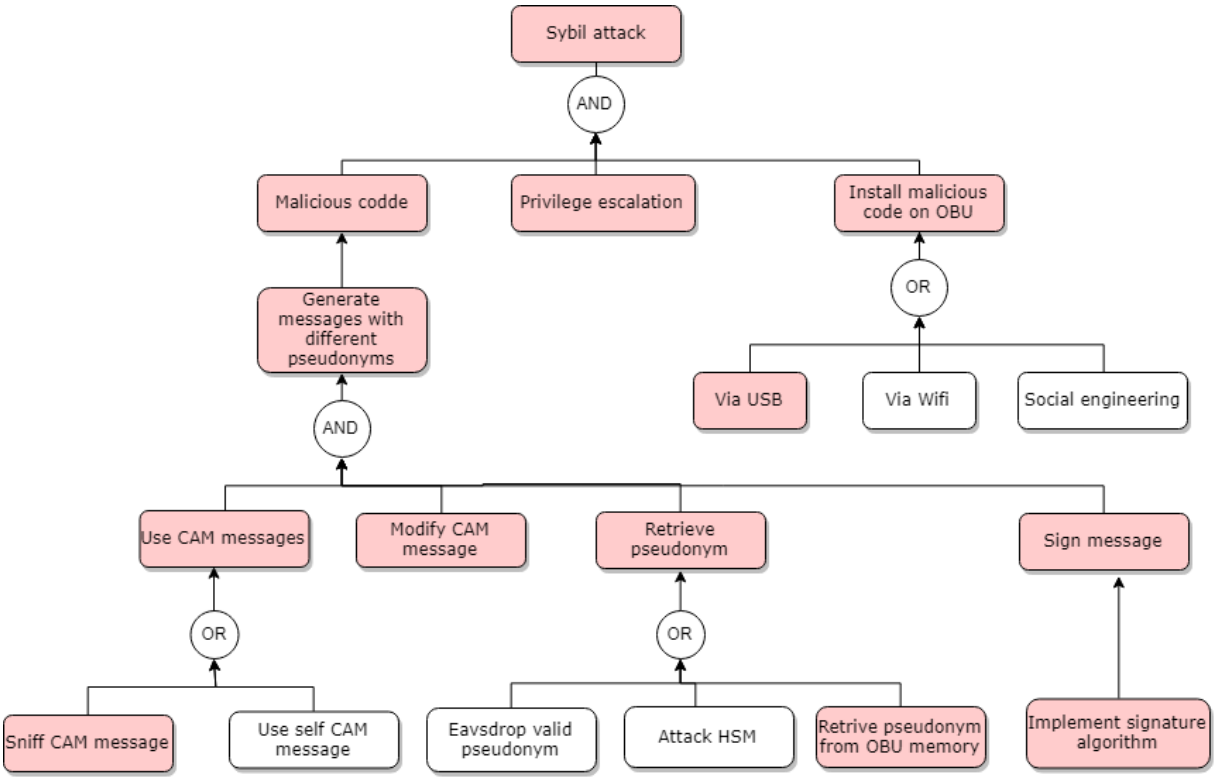

Figure 6.5: Sybil attack tree

3. After finishing the CAM modification (or new CAM generation), we retrieve pseudonym that we will use to sign the CAM message. The pseudonym can be stored on an Hardware Security Module (HSM) or on OBU memory. Other option is to steal valid pseudonym with their corresponding private key. We then sign the CAM with the pseudonym by implementing a signature algorithm.

The second step is privilege escalation. We used 'dirty COW' tool to change root password and execute our malicious code.

The third step is to install the malicious code on OBU. This can be done via different interfaces (e.g USB or wifi), or using social engineering method.

Figure 6.6 presents our setup. We dispose two OBU (YoGoKo unit) that communicate using ITS-G5. The attacker vehicle is the vehicle we have access to install the malicious code. We launch attack on attacker vehicle. We can view exchanged messages on ITS-G5 network using Wireshark. On the victim side, we visualize the results (ghost vehicle creation).

6.1.3.2 Results

Figure 6.7 presents the traces of Sybil attack execution on the attacker vehicle. Traces show that the MAC address, geonet, station ID, and the generation time are successfully changed. In order to validate that the victim vehicle will use the new addresses we should verify step 2 and step 3 presented in figure 6.6.

Step 2: we used Wireshark to visualize exchanged messages on ITS-G5 network. The Wireshark logs show our created CAM message presented in figure 6.8. We can see the CAM message created by the Sybil vehicle containing the same addresses.

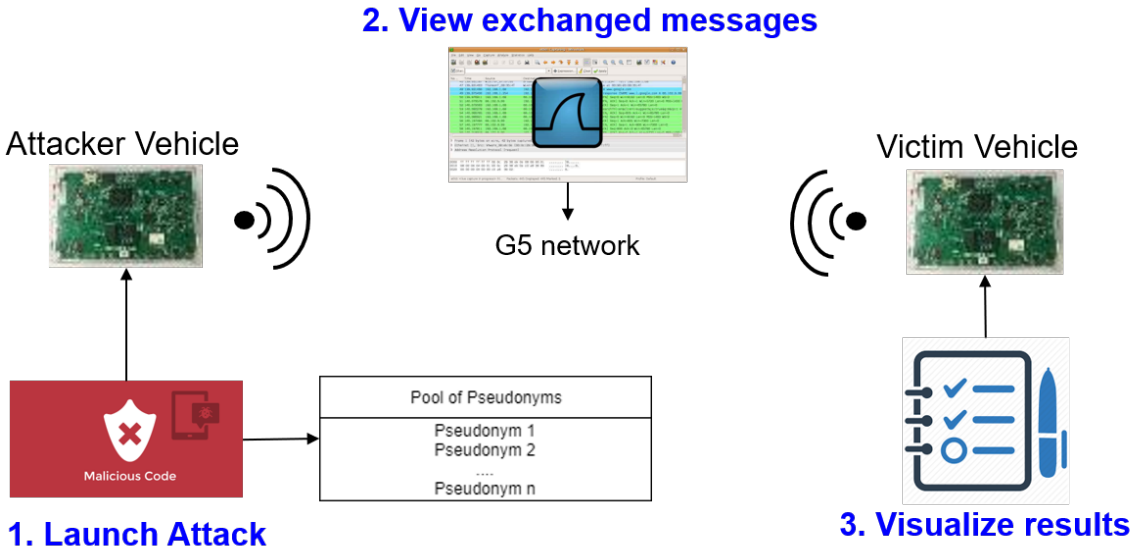

Figure 6.6: Sybil attack setup

```
root@YBOX-VEHI-1603-54137F(rw):~$ python3 sybil.py
Start Changing Mac address..... done  ----->  New Mac Address is  2a:5b:b0:96:7a:e3
Start Changing GN address..... done  ----->  New GeoNet Address is  00002a5bb0967ae3
Start Changing Station ID..... done  ----->  New StationID is  4177927816
Start Updating Generation Delta time field..... done  ----->  New Generation Time is  23643
Now data to be signed is ready
Start Signing Message..... done
.
Sent 1 packets.
```

Figure 6.7: Successful Sybil traces

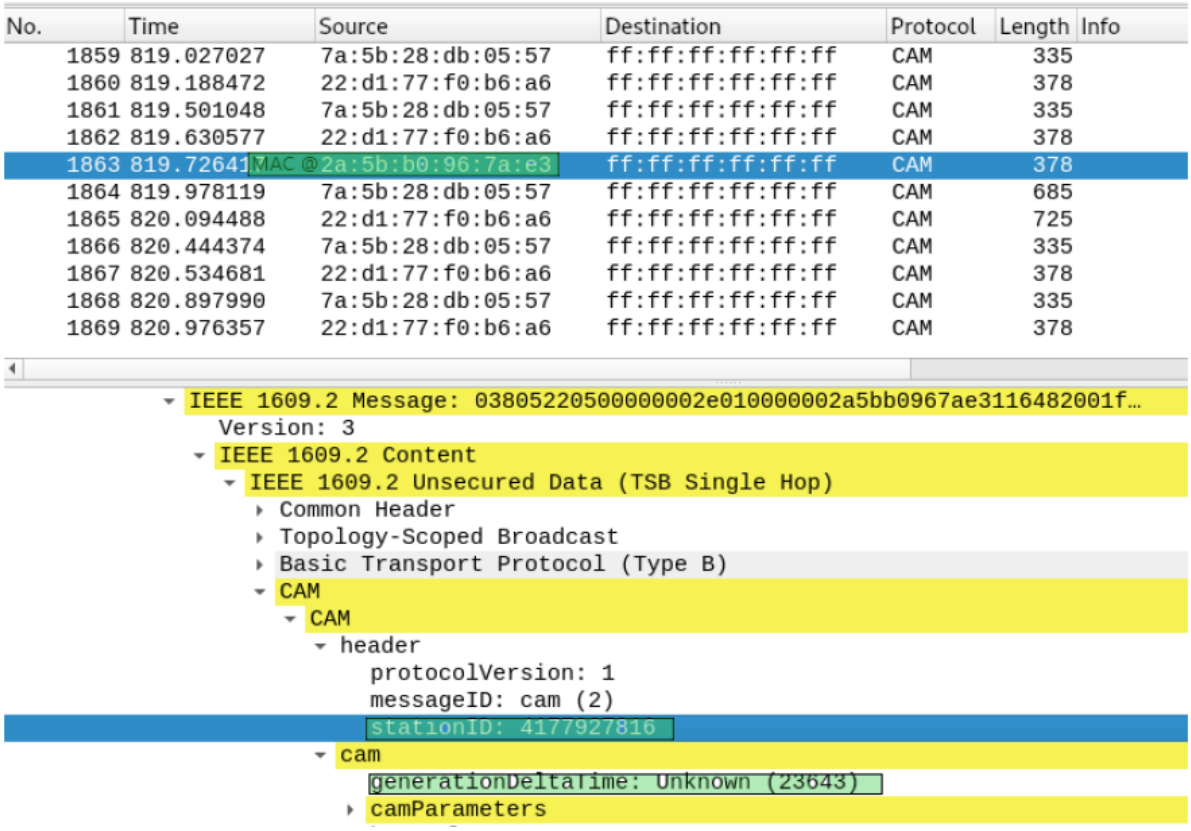

Figure 6.8: Wireshark of exchanged messages between attacker and victim

Step 3: Visualizing the results by visualizing the Local Dynamic Map (LDM) of the victim vehicle. The LDM is a conceptual data store located within a vehicle containing information which is relevant to successful operation of ITS applications and information on real-world and conceptual objects that have an influence on the traffic flow. Data can be received from a range of different sources such as vehicles, infrastructure units, traffic centeres and on-board sensors, for example received CAM from other vehicles are stored in the LDM. This enables the vehicle to have a clear vision on neighboring vehicles. Figure 6.9 presents the LDM of the victim vehicle that contains 3 objects: the vehicle itself, the malicious vehicle that initiates the attack and the ghost vehicle created by the Sybil attack. Storing the message in the LDM means that the message has successfully passed through all the checks and layers (including security).

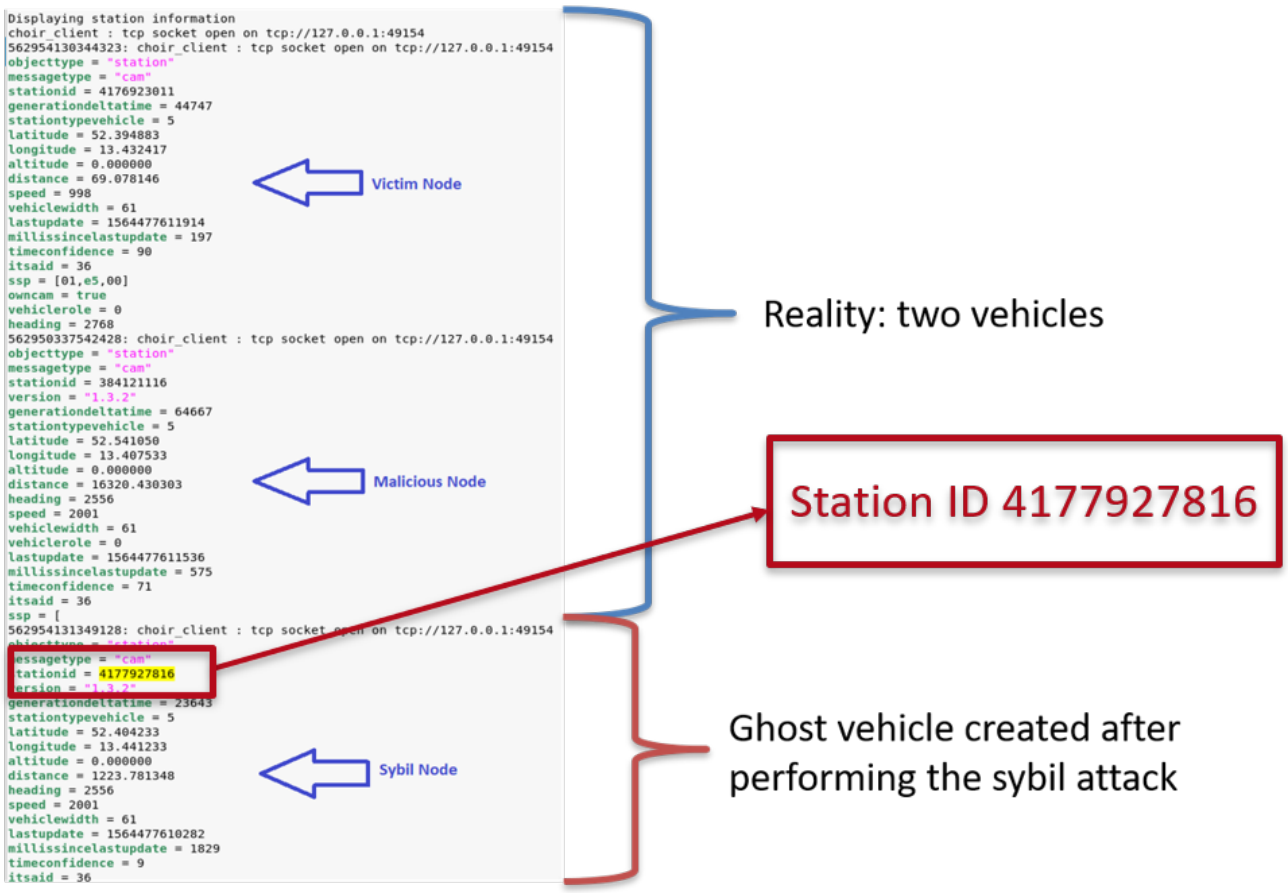

Figure 6.9: Local dynamic map (LDM) of the victim vehicle

Sybil attack is a very powerful attack since it can harm the overall system credibility. Comparing the sensors or cameras information with the LDM information can not fix the problem of sybil attack. Vehicles sensors information may be considered untrusted in case of technical sensor failure or broken equipment (sensor, camera, etc ...). In this thesis, we propose a detection mechanism based on global detection. It takes into account CAM's plausibility and reports misbehaving entities to a centralized entity. Detection mechanism is presented in the next section.

6.1.4 Sybil attack detection

Projects, consortium and standardization bodies are conscious of the importance of misbehaviour detection. In this section, we presents the general misbehavior detection process proposed by SCA project. This proposition is under revision to be included in ETSI standard.

6.1.4.1 General misbehavior detection process

The misbehavior detection process proposed by SCA project consists of the following operations:

1. The misbehavior detection: OBU and RSU locally detect a potential misbehaving entity. The ITS-S will keep checking the plausibility and the consistency of several mobility information in the V2X message until one check fails the tests. These local detection checks are detailed in section 6.1.4.2.

2. The misbehavior reporting: when an ITS-S detects a malicious behavior, it sends a Misbehavior Report (MR) to alert the Misbehavior Authority (MA) about the existence of a malicious entity in the network. The MA is a central authority located in the cloud, which is in charge of receiving and processing the MR.

3. The misbehavior investigation: the MA processes the received MR in order to detect the type of the reported misbehavior. The global detection of Sybil attack requires linking between several pseudonyms to identify the original attacker generator. The American architecture integrates a Linkage Authority (LA) entity whose function is to provide the results of linking several pseudonyms based on a straightforward association between them. However, a similar function does not exist in the European standards. Therefore, without prior knowledge on pseudonyms association, we specified an LA -like function based on ML technique to link several pseudonyms. This operation is detailed in section 6.1.4.3.

6.1.4.2 Local detection checks

The misbehavior detection process is largely based on checks performed by the ITS-S. Therefore, these checks should contain relevant and sufficient information for the detection process. In this thesis we used the implemented checks in multiple local detection works by Steven et al. [55] and Kamel et al. [56], all the implementations are open-source on github [57].

- *Range, position, and speed plausibility:* it tests if the position of the sending ITS-S is inside of the ITS-S maximum radio reception range, if it is plausible place (e.g. on a road, without overlaps of physical obstacles, etc.) and if the speed is plausible.

- *Position, speed consistency, and Position heading:* tests the distance separating two consecutive CAMs from the same ITS-S is less than a predefined maximum threshold. tests the plausible acceleration or deceleration, and tests the Position heading between two consecutive CAMs from the same ITS-S.

- *CAM frequency:* the time separating two consecutive CAMs from the same ITS-S is compliant with the standards.

- *Sudden appearance:* The CAM of a suddenly appearing ITS-S within a certain close range must not have a preset positive speed.

6.1.4.3 Misbehavior Authority investigation process

We used the Misbehavior Authority (MA) system architecture (see figure 6.10) proposed by Kamel et al.[58]. Our contribution consists of integration of the Sybil attack detection mechanism (by Sybil type) on the overall detection system. The architecture consists of three main phases: *General Misbehavior Type Detection*, *Pseudonym Linkage* and *Sybil Type Detection*. The MA system takes a Misbehavior Report (MR) as input and returns the predicted attack type as output. In the first phase, the general MD starts by detecting misbehavior types related to one single pseudonym identity. This detection is effective against misbehavior types that are non-Sybil. However, this detection fails against attacks that makes use of multiple pseudonyms. To address this problem we propose the pseudonym linking schemes of phase 2. In the second phase, we attempt to link the pseudonyms related to the same physical reported ITS-S. If no link is found, the process is complete and the misbehavior type is returned. If a link is found, then a Sybil attack is suspected and the linked pseudonyms are candidates for Sybil attack type detection in phase three. In this third phase the linked pseudonyms are treated as one and the evidences collected from all the linked pseudonyms is used in a specific Sybil type detection process. The predicted Sybil misbehavior type is returned, and the process is complete. The details of each phase are described below:

6.1.4.4 Phase 1: General Misbehavior Type Detection

The goal of this phase is to detect as accurately as possible the type of misbehavior related to one pseudonym as proposed by Kamel et al. [56].

6.1.4.5 Phase 2: Pseudonym Linking

This section presents our contribution, it consists of the linkage between pseudonym certificates used to perform attack, which means the detection of Sybil node. The goal in this phase is to link the pseudonyms coming from the same vehicle as accurately as possible. However, in order to be compliant with both US and European C-ITS Systems, we compare two options for pseudonym linking, linkage authority used in US (LA) and our Machine Learning based linking (ML based linking):

1. Pre Processing:

    - Space-Time selection: in this step, we propose to use the spatial database to recall all the reports within a range and time of the reporter node.
    - Prediction Filter: we use the output prediction of the phase 1 to filter reports with diverging predictions. If we detect (in phase 1) that the same type of attack for two different pseudonyms in the same region and type, we consider them candidates for linking test. Otherwise, the pseudonyms are discarded.
    - Autoencoder Distance Filter: we use the output prediction of the auto-encoder to filter reports with diverging compressed features. We calculate distances between the compressed features

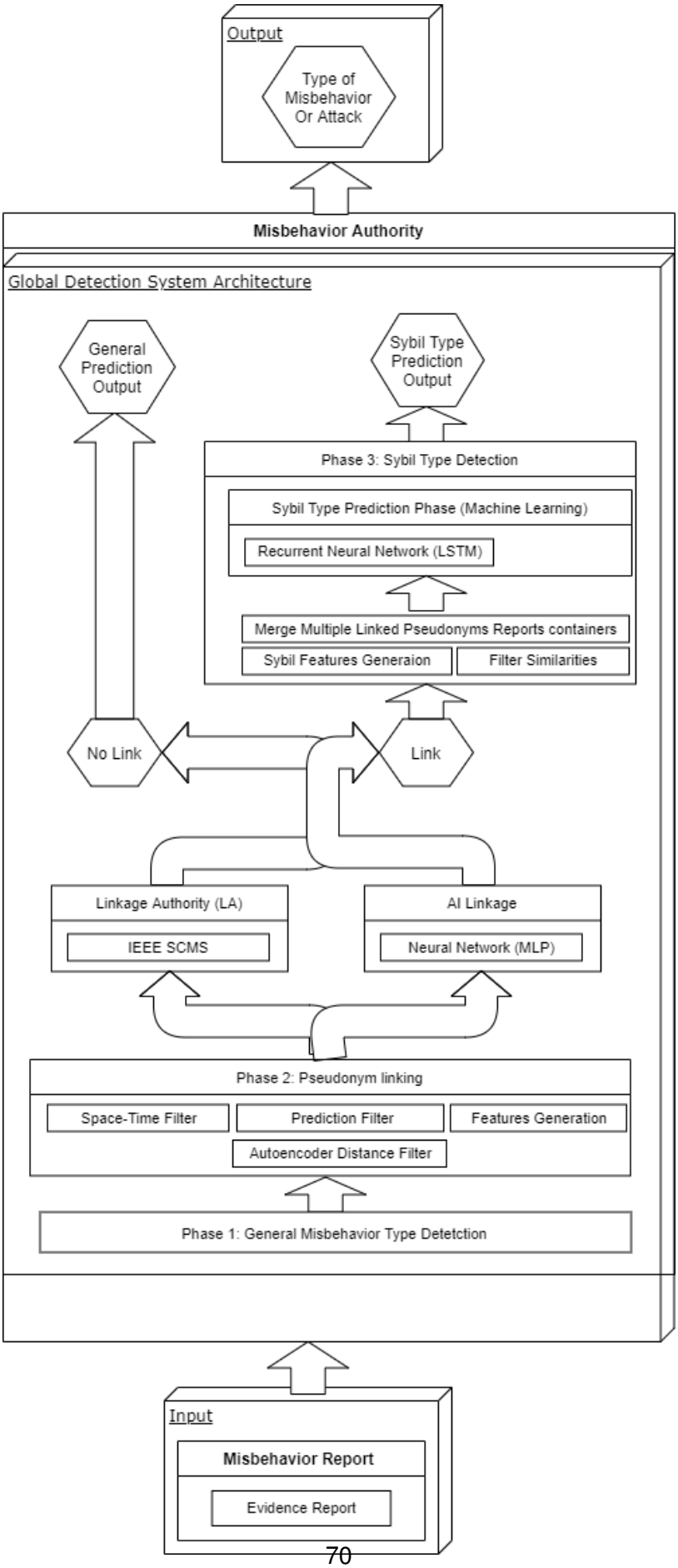

Figure 6.10: Global Detection System Architecture

of the recalled and current pseudonym. We exclude the pseudonyms with compressed features far from the one.

- Linkage Features Generation: similarly to the first feature generation step, we need to extract the relevant information from the selected pair of pseudonyms. These features are used by the ML algorithm to determine if the reported pseudonyms are linked or not. Therefore, we extract and validate the following set of features from each pair of reports:
  - The difference between all the previously calculated features of the two latest received reports of each pseudonym.
  - The euclidean distances between the reporter ITS-S position and broadcasted position of the reported pseudonym for both selected pseudonyms.
  - The euclidean distances between the reporter ITS-S position of one pseudonym and the broadcasted position of the other reported pseudonym.
  - The absolute difference between the two latest RNN predictions of the selected pseudonyms.

2. Linking:

   - LA (Option 1): the US architecture supports a LA. This enables us to do straightforward linking between the selected pseudonyms. No ML-based prediction is needed.
   - ML-based linking (Option 2): the European architecture lacks a LA. To cope with this issue we propose using a ML-based solution. The goal of this solution is to determine, using the previously calculated features, if two reported pseudonyms are generated by the same physical vehicle. For testing purposes, we use an MLP, which is the classical type of neural networks.

6.1.4.6 Phase 3: Sybil Type Detection

This algorithm activates if a link is found in the previous phase. The goal is to detect the type of Sybil attack (presented in section 6.1.1) related to the number of linked pseudonyms in the previous phase.

1. Sybil Algorithm Pre-Processing:

   - Merge Multiple Linked Pseudonyms: in this step we prepare a new database entry where we merge the evidence data of the multiple linked pseudonyms.
   - Filter Similarities: similarly to the previous filter, we aggregate similar data from the new database entry. This also improves the prediction performance.
   - Sybil Features Generation: We extract from the new and filtered database entry the key detection information. These features are the indications used by the ML algorithm to determine the type of Sybil attack. We create the same features used by the general algorithm described in the first phase. Additionally, we add two specific feature to the Sybil type detection:
     - The number of linked pseudonyms.
     - The number of reports in the new database entry.

2. Prediction:

- RNN: we provide the previously calculated features to an RNN. We also use the LSTM for testing purposes.

Finally the output of the MA algorithm is the *Sybil Attack Type* if a pseudonym link is found and the *General Misbehavior Type* otherwise.

6.1.4.7 Simulation settings and scenarios

In order to evaluate our proposed solution, we use the F^{2}MD framework [59]. F^{2}MD is a VEINS extention, VEINS [60] is an open source framework for vehicular network simulations. VEINS is based on OMNeT++ and SUMO, a network simulator and road traffic simulator respectively. We use the LUST scenario for the vehicle traces [61]. LUST is a synthetic data set generated with SUMO and validated with real data, provided by the vehicular lab of the university of Luxembourg [62]. We use different sections of the scenario for the training part and testing part of our ML algorithms (Figure 6.15). The train scenario is $6.51km^2$ and of peak density of $104.5Vehicle/km^2$. The test scenario is $1.61km^2$ and of peak density of $67.4Vehicle/km^2$. The topology of the scenarios consists of a downtown area, with residential roads and main arterial roads linked to highways. In total, the train scenario contains $82,146$ vehicles with $301,082,858$ exchanged V2X messages and $5,209,072$ transmitted MR. The test scenario contains $24,663$ vehicles with $17,051,860$ exchanged V2X messages and $294,160$ transmitted MR. Both scenarios have an attacker rate of 5%.

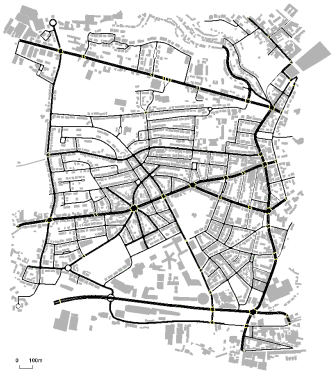

Figure 6.11: Test Network

Figure 6.12: Train Network

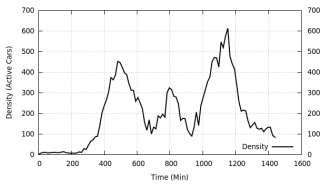

Figure 6.13: Test Vehicle Density

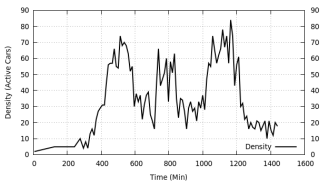

Figure 6.14: Train Vehicle Density

Figure 6.15: Simulation Scenario: Part of Luxembourg city

In both scenarios we implement the attacks described in section 6.1.1. Additionally, we used a set of other types of misbehavior implemented by kamel et.al [56], in order to increase the complexity of the classification. The misbehavior types are extracted from the literature [63]: (1) *Fixed Position Offset:* the

vehicle broadcasts its real position with a fixed offset, (2) *Random Position Offset:* the vehicle broadcasts its real position with a random offset limited to a max value, (3) *Fixed Speed:* the vehicle broadcasts the same speed at each beacon, (4) *Fixed Speed Offset:* the vehicle broadcasts its real speed with a fixed offset, (5) *Random Speed Offset:* the vehicle broadcasts its real speed with a random offset limited to a max value.

6.1.4.8 Results and analysis

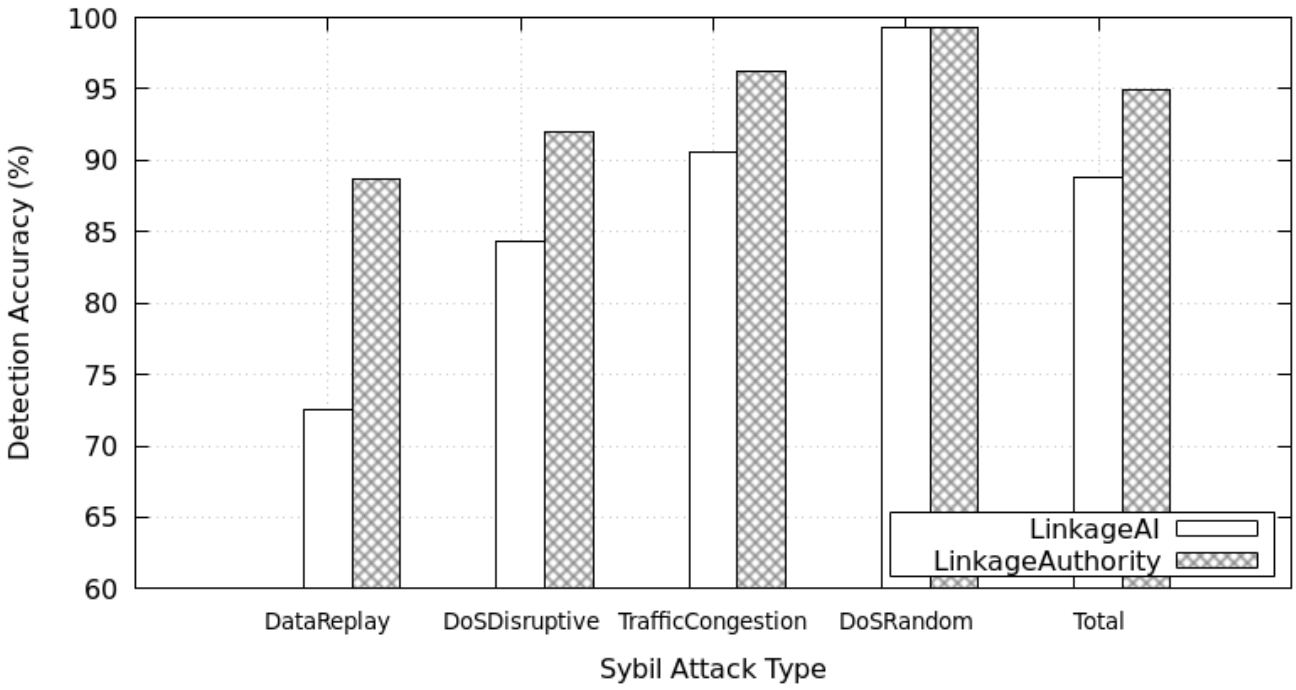

Figure 6.16: Detection Accuracy by Type of Linkage

Figure 6.16 shows the results of detection accuracy of the Sybil attacks by linkage type. The detection accuracy is the ratio of the correctly classified reported vehicles over all the reported vehicles. The first result we notice is that the total detection of Sybil attack types using a LA is at 94.97%, whereas it's at 88.83% when using the ML-based Linkage model. This is an expected result as the ML prediction is uncertain compared to the absolute information provided by the LA. We also notice that the detection accuracy difference between the two linkage types is proportional to the general detection accuracy for each type of Sybil attack. This is due to the prediction output of the first phase. Attacks that are difficult to classify, are less likely to be linked by the ML based Linkage. Especially since the classification output of the first phase is used as an input feature for the ML model. This problem however is not present using the ML.

Figure 6.17, Figure 6.18, Figure 6.19, and Figure 6.20 show the detection accuracy of Sybil attack (4 types presented in section 6.1.1) by the number of the received reports. In other words, it shows the number of reports needed for an accurate detection.

First, we notice that the detection accuracy for the *Data Replay Sybil* and *Dos Disruptive Sybil* attacks require more reports to converge than for the *Traffic Congestion Sybil* and *Dos Random Sybil*. The

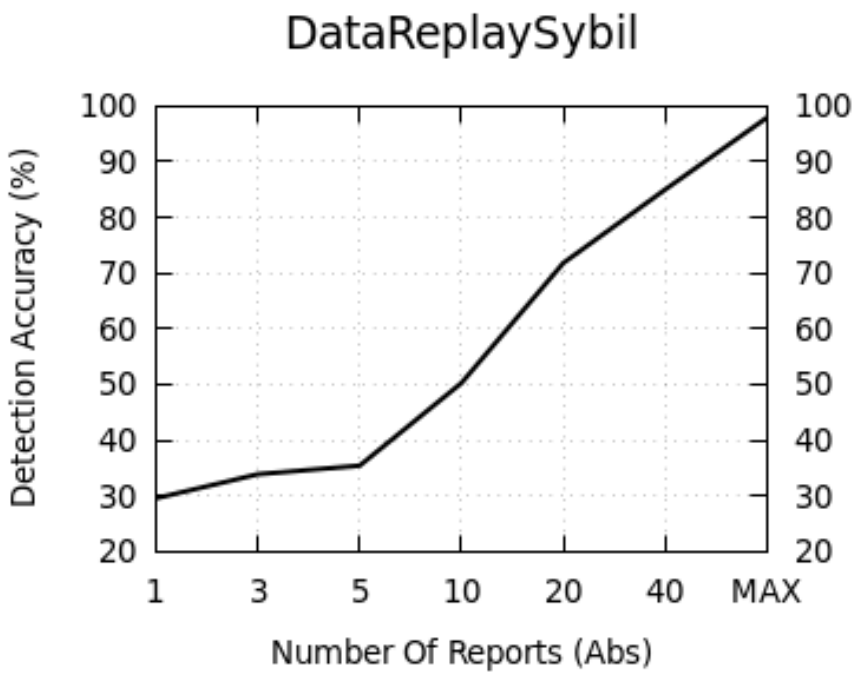

Figure 6.17: Detection accuracy of Data replay Sybil per number of received reports

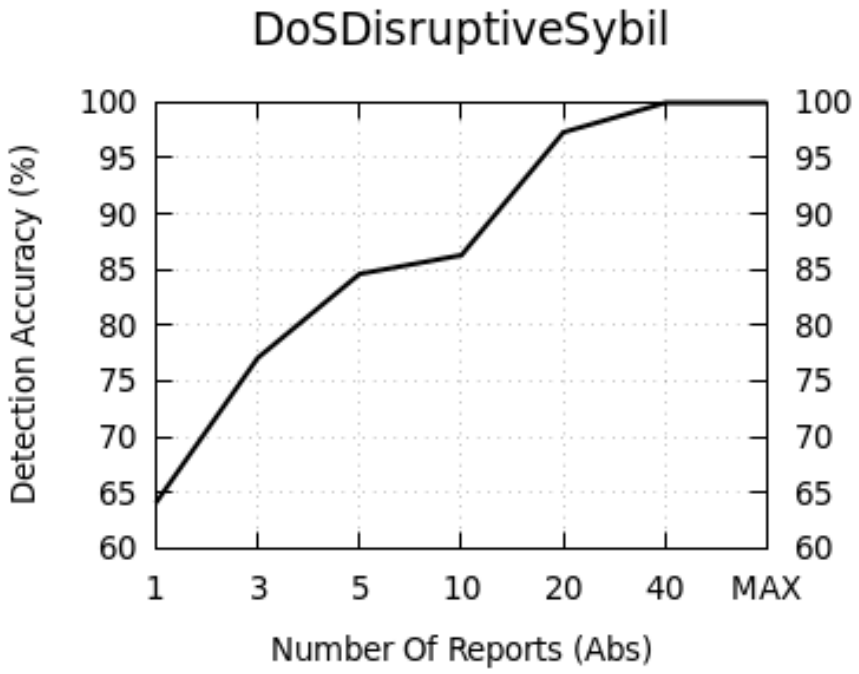

Figure 6.18: Detection accuracy of Dos disruptive Sybil per number of received reports

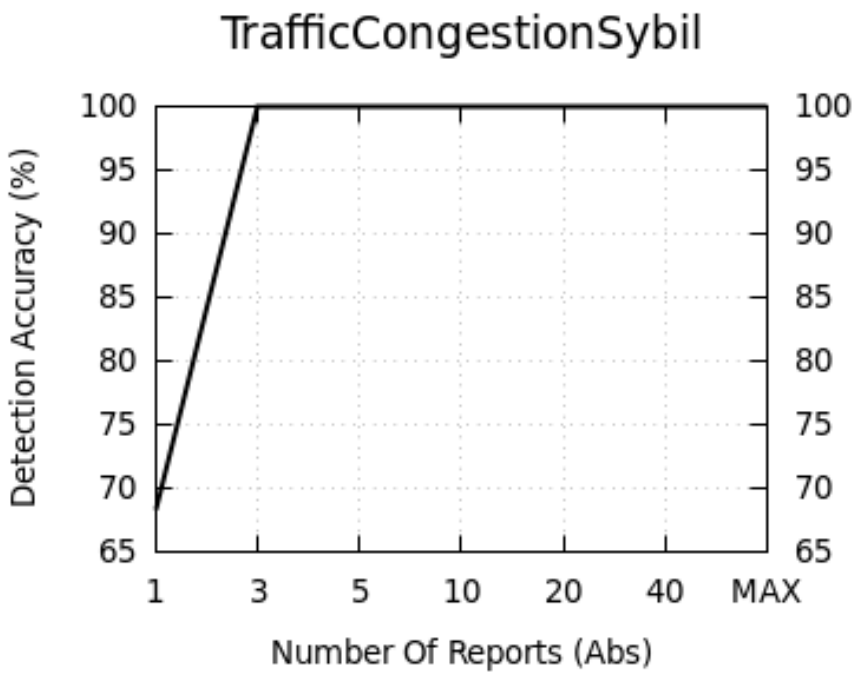

Figure 6.19: Detection accuracy of traffic congestion Sybil per number of received reports

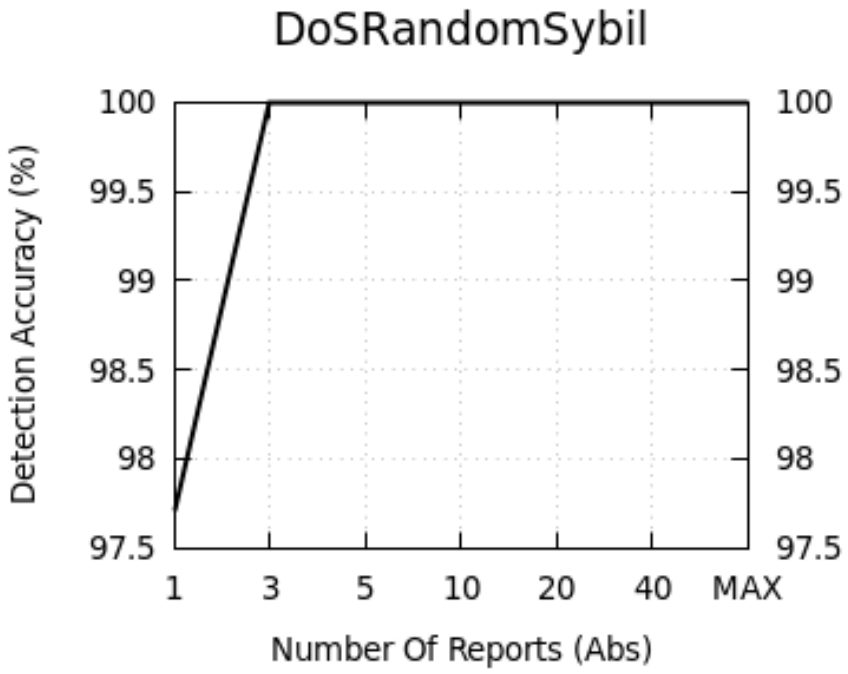

Figure 6.20: Detection accuracy of Dos Random Sybil per number of received reports

reasoning for that is that both former attacks cause the local vehicles to simultaneously report other genuine vehicles alongside the attacker. These false positive reports adds a significant amount of noise to the data. Therefore, more data is required to sort the genuine pseudonyms from the attacker pseudonyms. We also notice that the *Data Replay Sybil* attack requires more information than the *Dos Disruptive Sybil* to converge. This is a consequence of the former intelligently generating a realistic path instead of just replaying data incoherently.

Additionally, we notice that *Traffic Congestion Sybil* has a relatively low detection rate with one report. However, even though the attacker tries to intelligently remain within the plausible range, the detection then quickly converges. This is due to the lack of the simultaneously false reported genuine vehicles. The information is clean from false positives thus multiple reports are analyzed much more efficiently.

Finally, the *Dos Random Sybil* attack does not cause false positives neither is it within the plausible ranges. As a result it is easily detected even with evidence from only one report.

6.2 Tracking attack

6.2.1 Tracking attack description

In order to preserve driver's privacy, standardization bodies propose to change intelligently [64] pseudonym certificates during vehicle trips. The level of privacy intrinsically depends on the pseudonym change strategy and the attacker model considered. Many strategies have been proposed, and recently the Car-2-Car Communication Consortium (C2C-CC) proposed a strategy that could be potentially used by automobile manufacturers that are members of the Car-2-Car.

6.2.2 Related works

Many pseudonym change strategies are proposed in the literature [65]. The simplest strategy is based on fixed or random parameters [66], such as time , number of transmitted V2X messages or distance. Due to the simplicity of this strategy, an eavesdropper can easily guess the value of the used parameter and then link pseudonyms.

Pseudonym change strategy based on Silent period [67] means that the vehicle should stop sending any beacon messages for a certain amount of time. The silent period comes after a pseudonym change in order to make the prediction of the vehicle's position much more difficult. If the silent period is very short, the linkage of pseudonym is still feasible. However, using a long silent period can impact the safety applications because the vehicle is not allowed to send any V2X message. In some context, changing pseudonyms and entering a silent period is useless, e.g when the vehicle is alone on the road.

Karim et al [68] propose a location privacy scheme that lets the vehicle decide when to change its pseudonym and enter a silent period and when to exit from it adaptively based on its context.

Another concept is the mix-zone, it has been firstly proposed by Beresford et al. in [69]. This strategy consists of changing pseudonyms on a predefined road area. This creates an area where all nodes within it are ”mixed” as they are in silent period at the same time, such that it becomes very difficult for a tracker to determine where and when the node he is currently tracking will leave the mix-zone. Freudiger et al.

[70] studied the effectiveness of the mix-zone approach. Results show that the tracking success is related to the vehicle density.

The pseudonym change strategy recommended by the SAE J2735: [71] consist of changing pseudonyms every 120 s followed by a random silent period duration that vary from 3 to 13 s. The PRESERVE project evaluated the impact of privacy (i.e. pseudonym change) on an intersection collision avoidance system [72] [73]. Results show that the SAE J2735 [71] recommendation provides a decent privacy but drastically decreases safety.

Bjorn Wiedersheim et al. [74] evaluate an approach consisting of using new pseudonym for each sent message. Results show that vehicles can be tracked 80% of the time in medium vehicle density and 70% of the time in high vehicle density. Forster et al. [75] compare the average of pseudonym certificate used by trip using different type of pseudonym change strategies such as cooperative strategy, mix-zone, periodic etc. Emara et al. [76] assume a totally anonymous beacon message and proposes a vehicle tracker. Results show that the tracking is accurate (more than 90%) regardless of the entrance rate for less noisy positions for urban and highway scenarios.

Despite the number of pseudonym change strategies proposed in the literature, we do not know which strategy provides the best level of privacy. The pseudonym change strategy proposed by the Car2Car is one of the strategies that could be implemented by some car manufacturers. [77] is illustrated in figure 6.21 and consists of the following steps:

1. The first change (FC): A pseudonym change shall be triggered at the interruption of a trip which implies the end of a trip and the start of new trip. This condition is established by the following rules: engine control is deactivated for at least 10 minutes and engine control is activated and movement detection.

2. The second change (SC) shall be randomly performed during the trip in a range of 800 to 1500 meters from the start position.

3. The third change (TC) shall be performed at least 800 m from the last AT change and randomly within an additional interval of 2 to 6 minutes.

4. The fourth change (FOC) shall be performed after 10 kilometers or 20 kilometers (randomly)

5. Further changes (FTC) shall be performed after 25 kilometers and 35 kilometers (randomly)

The values used in this strategy have been obtained using traffic statistics presented in [78]. Traffic analyse of real German daily trip show that 95% of all trips are longer than 10 minutes or longer than 3 km.

6.2.3 Motivation

The General Data Protection Regulation (GDPR) addresses data protection as follows: Data in CAM messages are considered as private information, as vehicle's position and movement can be used to locate its driver, and any ITS-S in the transmission range can receive and use the CAM messages data.

A list of recommendations has been presented recently to the Commission which proposes to possibly add references to C-ITS and public transport, analyze in the next General Safety Regulation the need to

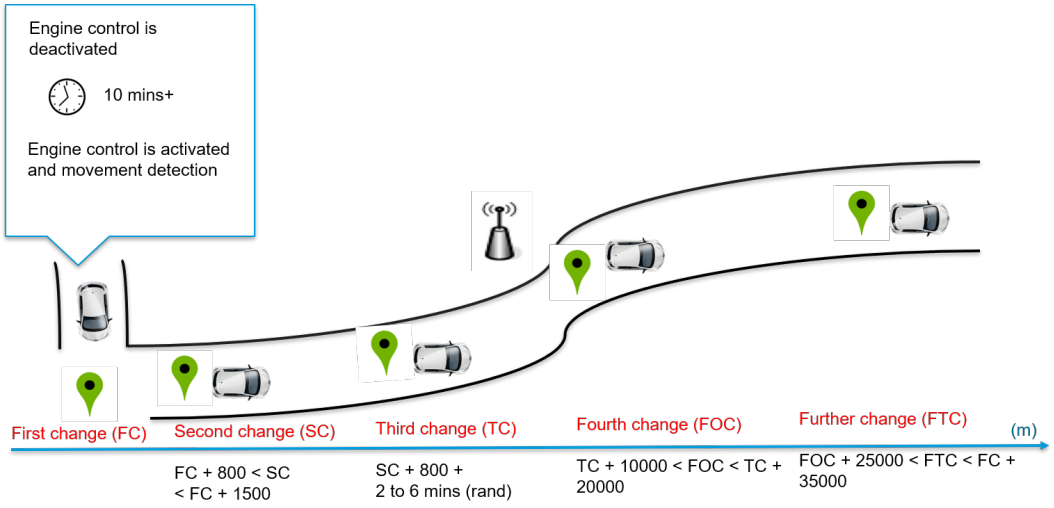

Figure 6.21: C2C Pseudonym change strategy

make C-ITS equipment mandatory in vehicles, taking into account the protection of personal data provided by the GDPR, the ePrivacy Regulation, the European Code of Electronic Communications and the Cyber-act in the C-ITS delegated act.

The pseudonym change strategy proposed by the Car-2-Car communication consortium is not well studied and evaluated in the literature. In this thesis, our contribution consists of privacy protection evaluation when using car-2-car pseudonym change strategy. Some modifications are proposed to improve this strategy.

6.2.4 Tracking attack feasibility

6.2.4.1 Attacker model

We study the problem of location privacy against two types of attackers: a mid-sized attacker (MSA) and a Global Passive Attacker (GPA).

- MSA does not have access to all exchanged messages but to a limited area only, for example, in a highway scenario he can cover 20, 30, 50 spots of 300 meter radius simultaneously. This can be the case of an attacker having installed antennas in interesting spots such as commercial urban zones.

- GPA can eavesdrop all exchanged CAM messages between vehicles all over a country. This attacker is less possible than a MSA since it will be financially impossible for someone to install antennas all over a country or a region to track vehicles. However, it could be feasible for an attacker who hacked the road infrastructure of a city.

6.2.4.2 Attacker success vs failure

Suppose that the attacker is trying to track *vehicle A*, the attack is considered successful in the following cases:

- If before silent period, the attacker tracked *vehicle A*, and after the silent period, the attacker can find the real position of *vehicle A*.
- If after a silent period the attacker is still able to successfully track *vehicle A* with few position missing (two to three positions for example).

If the attacker mixes vehicles and adds a wrong position to the track, meaning that he tracked *vehicle B* for some time, and after a while he found back *vehicle A*. In this case, we consider that the attacker has failed to track *vehicle A* and found it by chance.

6.2.4.3 Evaluation metric

The main objective is to evaluate the robustness of the pseudonym change strategy recommended by the Car2Car. The attacker estimates at each step the next position based on the last received CAM position or the last estimation if he did not receive any beacons (CAM) because of the silent period. However, when its estimation is too close to the real position, it is capable to construct the path of the tracked vehicle. On the other hand, the attacker may mix vehicle traces by mistake and assign a CAM to a wrong track. We define the following metrics:

1. Position error: consists of the difference between the real position of the tracked vehicle and the estimated position at each step. The position error is presented in equation 6.1.

$$\epsilon(t) = P_{real}(t) - P_{est}(t) \tag{6.1}$$

   Where $\epsilon(t)$ is the error at time t, $P_{real}(t)$ is the real position at time t, and $P_{est}(t)$ is the estimated position by the attacker at time t.

2. Probability of a vehicle to be not traceable after a pseudonym change. In other word the probability of an attacker to fail its attack and mix tracks.

6.2.4.4 Attacker algorithm

Our tracking algorithm, presented in Figure 6.22, consists of the following steps:

1. Initial state setup: attacker receives a CAM containing state information such as Pseudonym ID, position (X,Y), velocity, and heading.
2. Estimate next position: we propose two types of attacker, basic attacker and intelligent attacker. The basic attacker estimates the next position using the kinematic equations 6.2 and 6.3.

$$X_{t+\Delta_t} = X_t + \Delta t \times V \times sin(H), \tag{6.2}$$

$$Y_{t+\Delta_t} = Y_t + \Delta t \times V \times cos(H), \tag{6.3}$$

where X_t is the X position at time t, Y_t is the Y position at time t, V is the velocity at time t, and H is the heading. On the other hand, the intelligent attacker uses kalman filter to estimate or predict next position. Kalman filter steps are presented in section 6.2.5.

3. Create tracking window: the attacker creates a time tracking window (TW) using equation 6.4, it consists of the time interval where the vehicle may send the next CAM message.

$$IT + t_{min} < TW < IT + t_{max}, \tag{6.4}$$

where IT is the initial time, t_{min} is the minimum duration between two consecutive messages, t_{max} is the maximum duration between two consecutive messages according to the standards in Europe and US.

4. Compare pseudonym ID: the attacker parses the CAMs received during the tracking window. There are two possibilities: if the pseudonym ID (P_ID) saved during the initial state setup is equal to the P_ID in the CAM inside the tracking window, it means that the vehicle does not change its pseudonym ID. Then, the next step is step 5. Second case, if the pseudonym ID received in the last message (saved during the initial state setup) is different from the pseudonym ID in the received CAM. The next step is step 6

5. The attacker adds the position to the track.

6. If the received CAM contains a new pseudonym ID, the attacker considers two possibilities 1) the received CAM is for another vehicle, or 2) the vehicle changed its pseudonym ID. The attacker thus, should verify if the received CAM is in the plausible range of the tracked vehicle (SV on Figure 6.23). The plausible range presented in figure 6.23, consists of two tests that should be done: 1) if the $estimatedposition - lastposition$ is less than a $threshold$. and 2) test if the heading of the received CAM is plausible (i.e we eliminate vehicles heading in the opposite direction).

7. Add to plausible list: if the received CAM is in the plausible range, the attacker add this position to the plausible list (list of potential candidates).

8. Move to the next received CAM.

9. End of TW?: Check if the received CAM is inside the current TW. If yes, go to step 4. Else, move to step 10.

10. Check if the plausible list is empty.

11. Choose the nearest position from the plausible list and add the received position in the track (go to step 5).

12. Consider that the vehicle is in a silent period and add the estimated position in the track (go to step 5). If the received CAM is not in the plausible range the attacker then parse all CAMs in the TW. A list of possible CAMs is created. At the end, the attacker should select the nearest vehicle from this list.

13. Update statement: Update the current position with the position contained in the selected CAM or in own prediction (in case of silent period) and move the tracking window.

6.2.5 Kalman filter

The Kalman filter process has two steps: the prediction step, where the next state of the system is predicted given the previous measurements, and the update step, where the current state of the system is estimated given the measurement at that time step. The steps translate to equations as follows:

1. Prediction step:

$$\mathbf{x}_k^- = A_{k-1}\mathbf{x}_{k-1} + B_k U_k \tag{6.5}$$

$$P_k^- = A_{k-1}P_{k-1}A_{K-1}^T + Q_{K-1} \tag{6.6}$$

2. Update step:

$$\mathbf{V}_k = Y_k - H_k X_k^- \tag{6.7}$$

$$\mathbf{S}_k = H_k - P_{k-1}H_k^T + R_k \tag{6.8}$$

$$\mathbf{K}_k = P_k^- H_k^T S_k^- \tag{6.9}$$

$$\mathbf{K}_k = P_k^- H_k^T S_k^- \tag{6.10}$$

$$\mathbf{X}_k = X_k^- K_k V_k \tag{6.11}$$

$$\mathbf{P}_k^- = P_k^- - K_k S_k K_k^T \tag{6.12}$$

where

- x_k^- and P_k^- are the predicted mean and covariance of the state, respectively, on the time step k before seeing the measurement.
- x_k and P_k^- are the estimated mean and covariance of the state, respectively, on time step k after seeing the measurement.
- Y_k is the mean of the measurement on time step k.
- V_k is the innovation or the measurement residual on time step k.
- S_k is the measurement prediction covariance on the time step k.
- K_k is the filter gain, which tells how much the predictions should be corrected on time step k.

6.2.5.1 Simulation and scenarios

We evaluated our hypothesis using traffic and V2V communication simulation. We used the open-source V2V simulator, VEINS [79].

VEINS allows the implementation of custom schemes for pseudonym change and silent period. We implemented the two following schemes for our evaluation:

- Car-to-Car pseudonym change scheme [77].
- Fixed time with random periodicity pseudonym change with fixed time-period silent period [64]: a vehicle starts its journey with an initial pseudonym certificate. During this journey, the vehicle changes pseudonym certificate at random periods in order to confuse the attacker.

We simulated two scenarios: the first one consists of 100 km straight highway (Figure 6.24) and a real road network from Brooklyn, New York, USA (Figure 6.25). We use medium vehicle density. Vehicle density is controlled using arrival time between two vehicles. Hence, arrival time for medium density is 1.5s. The frequency of CAM sending is 10 Hz.

6.2.6 Results and analysis

Figure 6.26 presents the position error for one fail and one success scenario. For the success scenario, the vehicle enters the simulation at time t = 59.9 ms, the error presented in equation 6.1 is equal to zero that means that the attacker can easily track the subject vehicle, at time t = 84.4 ms the error increases to reach 6.49. This is due to the entering of the vehicle in silent period for 1s, the attacker starts its position prediction until he finds the vehicle again. As we see, the error tends to zero at t= 84.5 ms, which means that the attacker re-finds the vehicle after the end of the silent period. In this case, the attacker is perfectly tracking the vehicle, and its estimation is close to the real position.

For the vehicle fail scenario, the vehicle enters the simulation at t= 43.88ms, the error starts increasing when the vehicle enters in the silent period at t = 65.38 ms until reaching 9.95 at t=67.18ms. It then decreases to 6.22 at t= 67.28ms, this is due to the attacker finding a vehicle's position close to its estimation. In this case, the attacker mixes the tracks and assigns the position of another vehicle to the track of tracked vehicle. The error stabilizes at 6.23 which means that the attacker is now tracking another vehicle that is 6 meters away from the subject vehicle.

6.2.6.1 Mid sized attacker

The attacker should install eavesdropping antennas all over the network to have full coverage of the exchanged messages. In this MSA model, we assume that we have multiple eavesdropping antennas, we run multiple simulations:

- MSA with 20 antennas.
- MSA with 50 antennas.
- MSA with 75 antennas.
- MSA with 100 antennas.
- MSA with 125 antennas.

The range of each antenna is 800m. The tests are run on highway scenario of 100 km. In 100km highway scenario, 125 antennas means a full coverage of the road. We considered a uniform distribution of antennas.

Figure 6.27 presented results of CDF of being untraceable versus the number of spots or antennas used by the attacker. Results present that the cumulative distribution function (CDF) of being untraceable is 1 when we cover 0 to 100 spots. This result is common for the two types of attackers (basic and intelligent KF). At 125 spots, the attacker became a global attacker, this means that it has access to all exchanged messages on this area. We see that the CDF of being untraceable is 0.009, which means that vehicles are traceable using both the basic and KF attacker. These results mean that even with an intelligent attacker, we are not able to track vehicles if we do not have access to all exchanged messages.

Figure 6.28 presents the prediction quality using the basic attacker and the intelligent attacker (KF attacker) on highway scenario. Results present that both are well predicted on a highway. For the basic attacker, after the second pseudonym change the prediction error increase to 0.6m. The KF is more efficient than the basic attacker where the prediction error is close to zero even after the pseudonym change. These results were expected because KF is more intelligent and takes into account the covariance error at each prediction step.

Figure 6.29 presents the prediction quality using the basic attacker and the intelligent attacker (KF attacker) on urban scenario. Results presents that the KF attacker is more efficient in urban scenarios because the prediction error is always close to zero. On the other hand, we can see that for the basic attacker the prediction error is increasing exponentially after each pseudonym change. The prediction error is important to present the robustness of the attacker model.

6.2.6.2 Global attacker

Global attacker have all the exchanged messages for all vehicles trips. We simulate the C2C strategy, but we add a scenario with different silent period duration (0,1,2 seconds). In the rest of this study, we use the basic attacker.

Figure 6.30 presents the cumulative distribution function (CDF) of being untraceable after a pseudonym change (PC) using car2car strategy on a Brooklyn grid scenario. When the PC = 0, no pseudonym change has occurred yet, the probability of being untraceable is zero for all silent period duration, which is logical because all vehicles are easily traceable without changing their pseudonyms. After the first pseudonym change (PC = 1), without silent period (0s) the attacker can easily link the messages coming from the same vehicle because he have all the exchanged messages. The probability of being untraceable has increased for the SP = 1s as well as for SP = 2s. The attacker can mix the track and loose the tracked vehicle after 1s and loose almost all the tracked vehicles after 2s of silent period.

Figure 6.31 presents the cumulative distribution function of being untraceable after a pseudonym change using car2car strategy on a highway scenario. Compared to the C2C grid scenario, the probability of being untraceable is smaller after the second pseudonym change, as the attacker can track more vehicles than the c2c grid scenario. This is logical because the tracking in a highway scenario is easier than the grid or urban scenario.

Figure 6.32 presents the cumulative distribution function of being untraceable after a pseudonym change using random pseudonym change strategy in an urban scenario. Results present that after the second pseudonym change the probability of being untraceable has increased to reach 0.74 for SP =

0s, 0.98 for SP = 1s and 1 for SP = 2s. This means that basic attacker has mixed tracks after the first pseudonym change.

Figure 6.33 presents the cumulative distribution function of being untraceable after a pseudonym change using random pseudonym change strategy on highway scenario. Results present that without silent period vehicles can be easily traceable. Using a silent period of 1s, the probability of being untraceable reaches 0.68 after the 7th pseudonym change. And reach 0.9 using the 1s duration, after the second pseudonym change.

6.2.7 Conclusion

Results show that a MSA (basic and intelligent) is not able to track vehicles using 25, 50, 75, 100 spots on a highway. A global attacker is able to track vehicles if they are using the two pseudonym strategies (C2C and random) without a silent period whether in a highway scenario or in an urban scenario. On the other hand, adding some silent period can improve the ability of the C2C pseudonym change strategy to guarantee vehicle's privacy.

We conclude that a global attacker is able to track a good percentage of vehicles no matter which pseudonym change strategy is used.

6.3 CRL substitution attack

6.3.1 Certificate Revocation List (CRL) substitution attack description

As the name implies, this attack tries to substitute existing CRL by another expired one. CRL, as defined in ETSI 102 941 [80], is a signed list indicating a set of certificates that have been revoked by the certificate issuer. The CRL contains:

- CRL version: the version of CRL certificate.
- ThisUpdate: this field indicates the issue date of this CRL.
- NextUpdate: this field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date.
- Entries: entries of revoked certificates.

The PKI broadcasts the CRL to all vehicles, this list should be updated and re-broadcasted whenever a new trusted entity is compromised. CRL distribution protocol is an ongoing subject in ETSI standard. After analyzing existing propositions, we found that CRL substitution attack is possible. Existing solution needs to be improved in order to deal with this attack.

Historically, substitution attacks were first introduced in encryption algorithms by swapping legitimate algorithm by compromised one that can monitor communication. In addition, it was exploited on key exchange and signature schemes. In the context of C-ITS, for the moment, ETSI standards specify just the verification of the CRL's issuer using RCA verification key. Then, ITS-S verifies only if the CRL is generated by the legitimate entity. Figure 6.34 presents the attack tree of CRL substitution attack.

6.3.2 CRL substitution attack implementation

For CRL substitution attack, we consider some hypotheses presented below:

- We consider one victim vehicle represented by one OBUs presented in section **??**. This OBU communicates over ITS-G5.
- Victim vehicle is an operable vehicle (i.e it have an enrollment certificate and a pool of valid pseudonyms).
- We are not using the HSM. Secret keys and pseudonym certificates are stored on the host CPU memory of the system.
- We dispose of a trace of expired CRL respecting the CRL format specified by ETSI standards.

As presented on the attack tree, there are two options to implement CRL substitution attack: Locally or remotely. Local method consists of developing and installing malicious code on the embedded OBU of the vehicle. As the CRL is signed by the RCA, the creation of new compromised CRL is not possible and will be rejected by the OBU when verifying the RCA's signature. In our attack implementation, we substitute the CRL by an expired one, which creates a real risk on the OBU trust communication. Attacked OBU may trust a revoked entity. The second step is to do privilege escalation. We used 'dirty COW' tool to change root password and execute our malicious code. Installing malicious code as described in the sybil attack tree can be done via multiple interfaces such as USB port, WI-FI or social engineering methods.

6.3.3 Results

From the trace of the security stack of the victim vehicle, presented in Figure 6.35, we can see that the generation time is the 1st of August 2019 at 13:16:37, which presents the *thisupdate* parameter of the CRL. The *nextupdate* is the 1st of August 2019 at 13:30:37. This means that a new CRL should be communicated by the RCA before the *nextupdate*. We performed the attack in 27 August at 13:10:12. The CRL used was expired when the attack was performed, as presented in figure 6.35. The expired CRL was successfully reloaded.

6.3.4 Proposed verification algorithm

In order to deal with this attack, we propose a verification algorithm. The diagram of the CRL verification is presented in Figure 6.36. When a vehicle receives a new CRL, it should verify CRL signature. If it is not valid, the vehicle should reject the received CRL. In the other case, the vehicle should verify if *thisupdate* is

- Plausible: which means that the date is not far in the future.
- The *thisUpdate* ¡ *NextUpdate* of the previous received CRL.

On the other hand, the vehicle should verify if *nextupdate* is not outdated.

6.4 Exhaust of pseudonym pool

In ETSI all received messages are signed in order to authenticate the sending vehicle. If vehicle's pseudonym pool is empty, the vehicle can not sign messages and thus will not send unsigned messages because they will be discarded. This is the vulnerability that we use in this attack. The idea of this attack is to force the vehicle to change their pseudonym certificate and thus exhaust its pseudonym pool.

6.4.1 Attack implementation

Figure 6.37 presents the attack tree for Exhaust pseudonym pool (EPP). To implement EPP attack we have two options: Locally or remotely. The local method consists of developing and installing malicious code on the embedded OBU of the vehicle. Remote attack consists of provoking geo-networking address collision. Eavesdropping CAM sent by the victim vehicle to extract geo-network address and create messages containing the same geo-network address and then broadcast it over the ITS-G5 network.

6.4.2 Results

As shown in the green box number 1 in Figure 6.38, the address of the victim vehicle is 2a:36:3b:70:1b:0e. The address is also shown in Figure 6.39 (highlighted in blue). After performing the attack, we can see in the green box number 2 in Figure 6.38 that the victim vehicle detects a duplicate address and triggers a pseudonym change from the pseudonym change module. The green box number 3 show the new address (8a:6c:8a:ac:3b:54) The results in the Wireshark of Figure 6.39, where the vehicle starts sending CAM messages using new pseudonym and new addresses (see the message directly after the highlighted blue message).

6.5 Conclusion

This chapter presents the implementation of the attacks found in the risk analysis. The attacks are: Sybil, tracking, CRL substitution, and exhaust of pseudonym pool.

For the Sybil attack, we first presented the feasibility on real equipment used in the SCA project. Results present that the Sybil attack is feasible if the attacker have access on pseudonym certificates and the corresponding private keys. Thus, the limitation of access to such keys can solve the problem. On the other hand, we proposed a detection mechanism to detect the Sybil attack using a global misbehavior authority investigation. Results present that detection depends on the Sybil attack type.

For the tracking attack, we proposed two attacker model (mid-sized and global). Results present that a global attacker can track vehicles, but adding some silent period can make the tracking much harder. For the MSA, we present that vehicles are not traceable using a basic and even an intelligent attacker (kalman filter based attacker).

For CRL substitution attack, we proposed an attacker that substitute the existing CRL with an expired one. Results present that the attack is feasible. We proposed a verification algorithm to deal with this attack.

For the Exhaust of pseudonym pool (EPP) attack, we demonstrated that this attack is feasible and the solution may be the prevention of changing identities when a collision is detected multiple times.

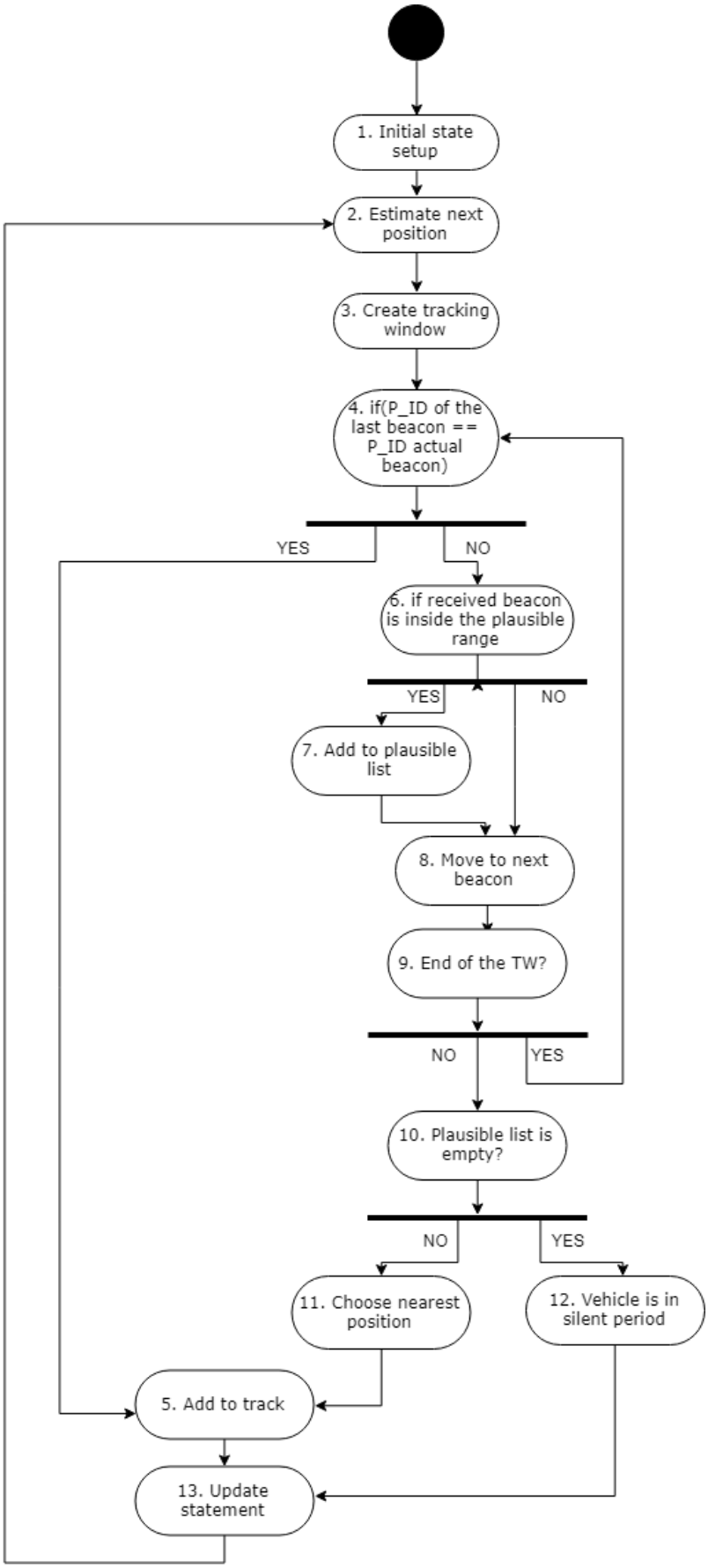

Figure 6.22: Tracking algorithm

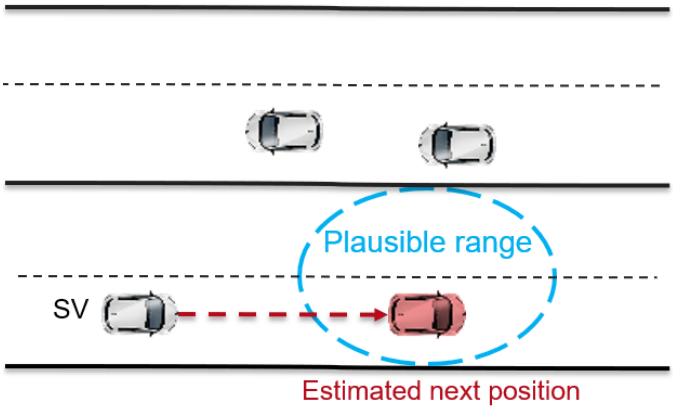

Figure 6.23: Plausible range

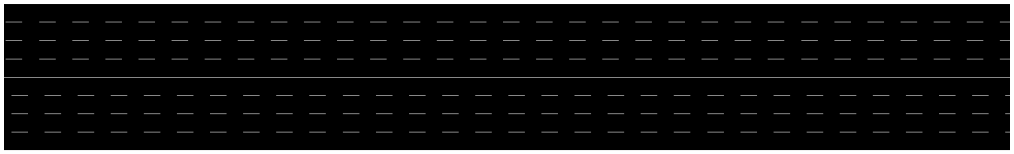

Figure 6.24: Highway scenario (100 km long), 4 lanes for each direction

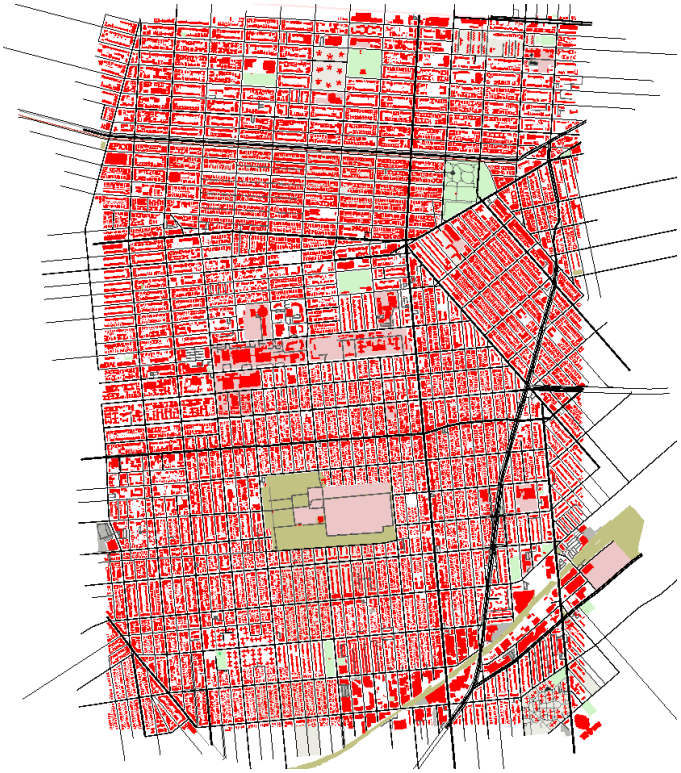

Figure 6.25: Brooklyn grid road network scenario

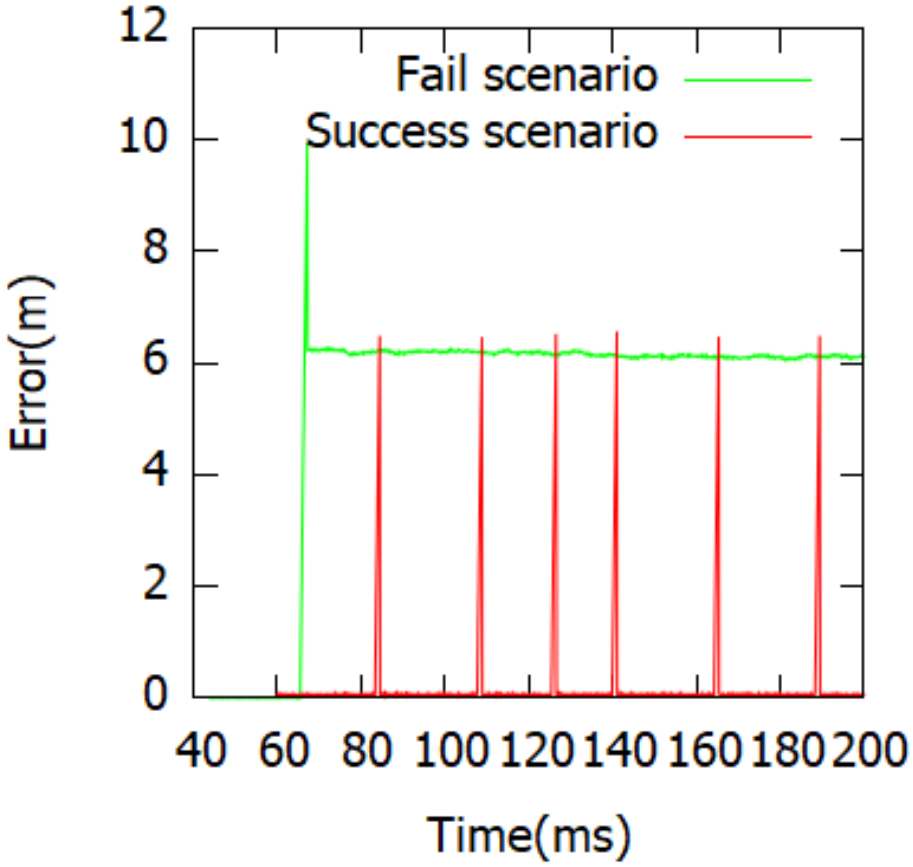

Figure 6.26: Prediction error for fail and success scenario

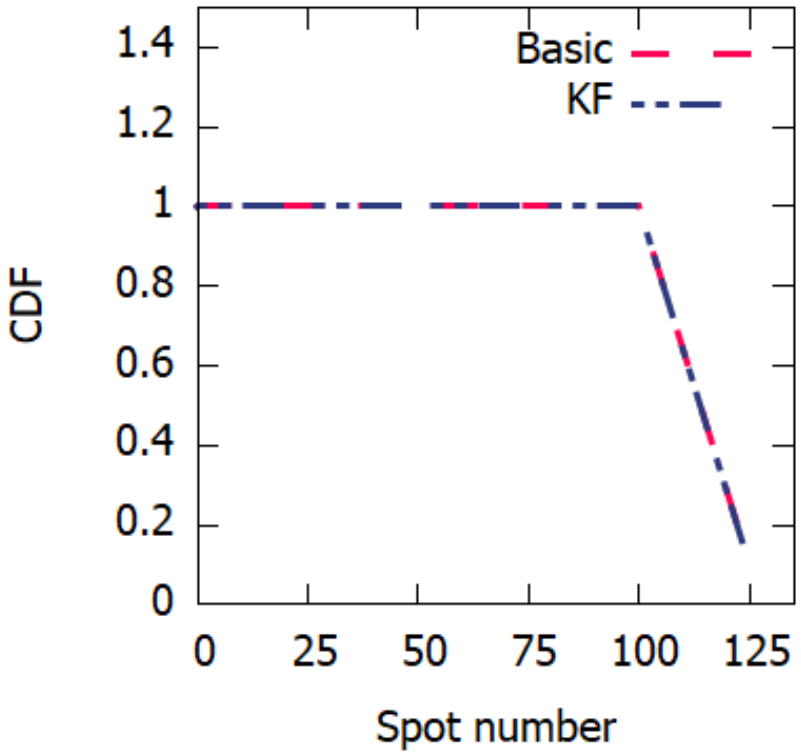

Figure 6.27: CDF of being untraceable vs number of attacker spots

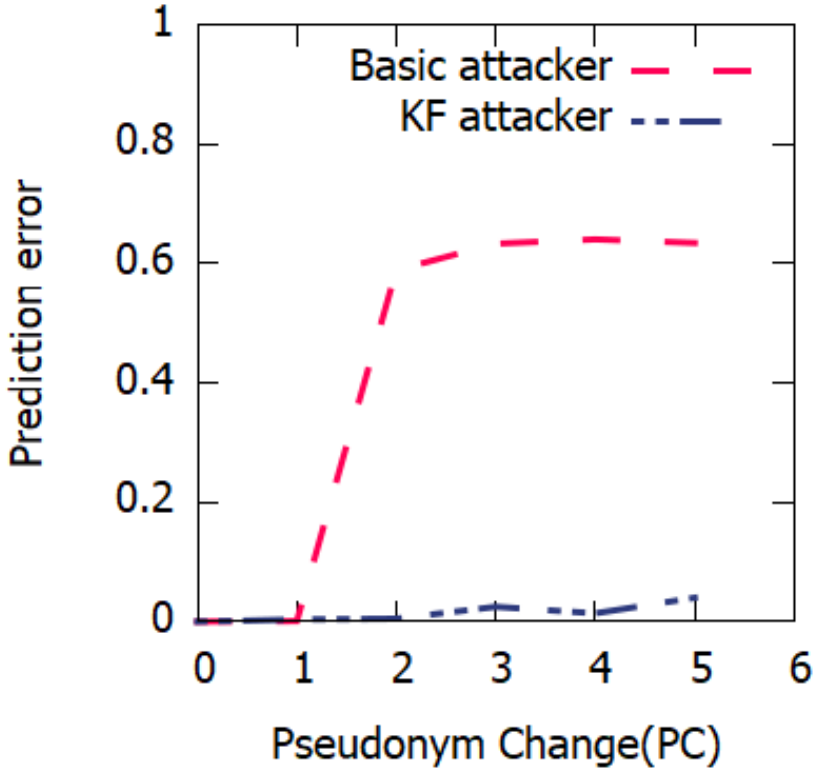

Figure 6.28: Basic vs kalman filter prediction quality on highway scenario

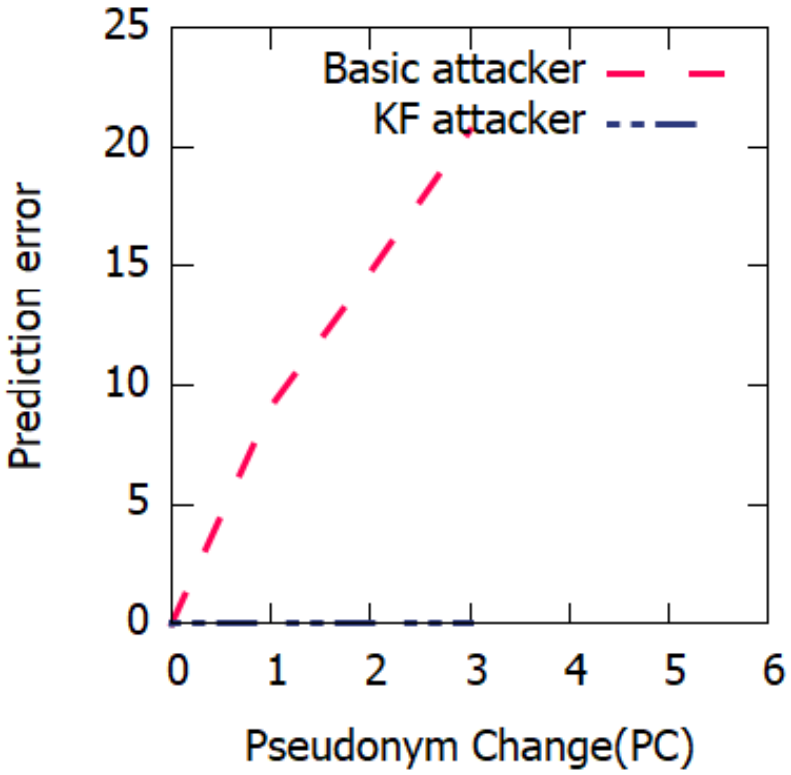

Figure 6.29: Basic vs kalman filter prediction quality on grid scenario

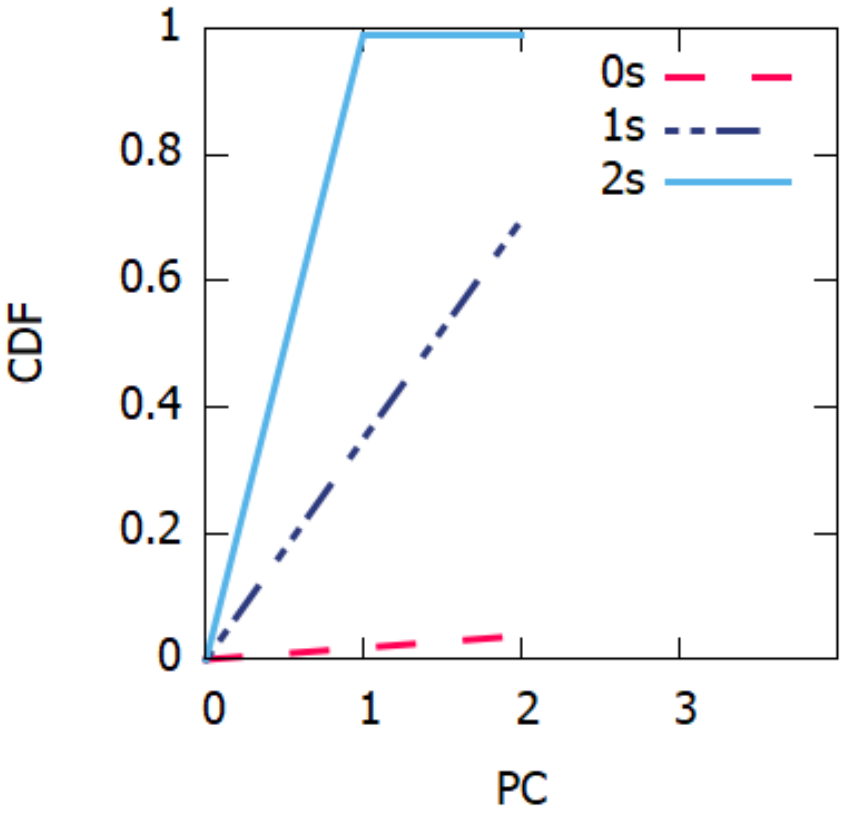

Figure 6.30: CDF Car2car grid scenario with different silent period duration (0,1,2 seconds)

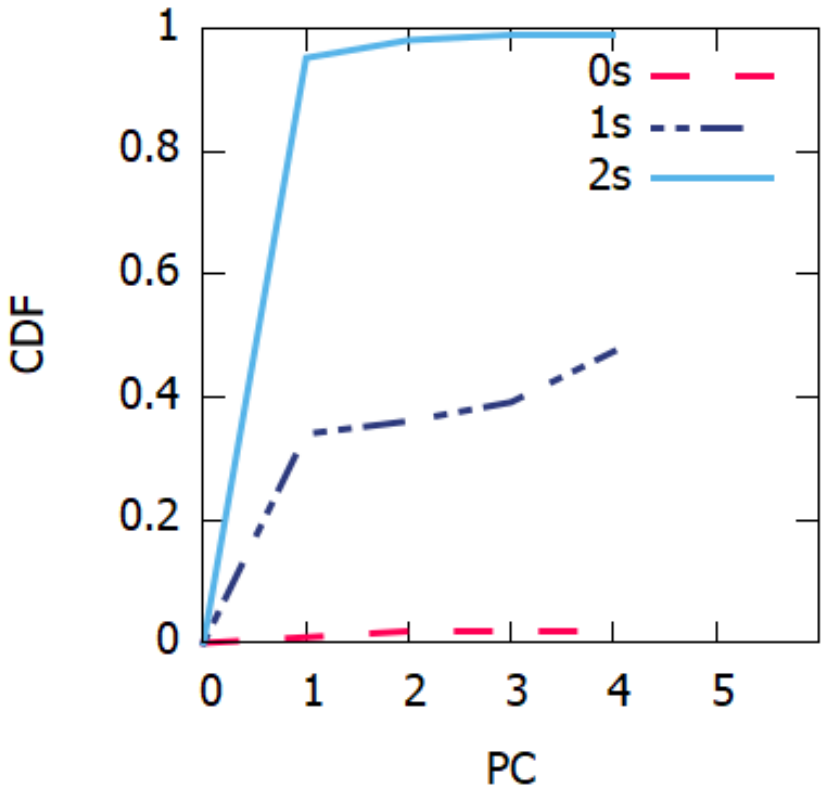

Figure 6.31: CDF Car2car highway scenario with different silent period duration (0,1,2 seconds)

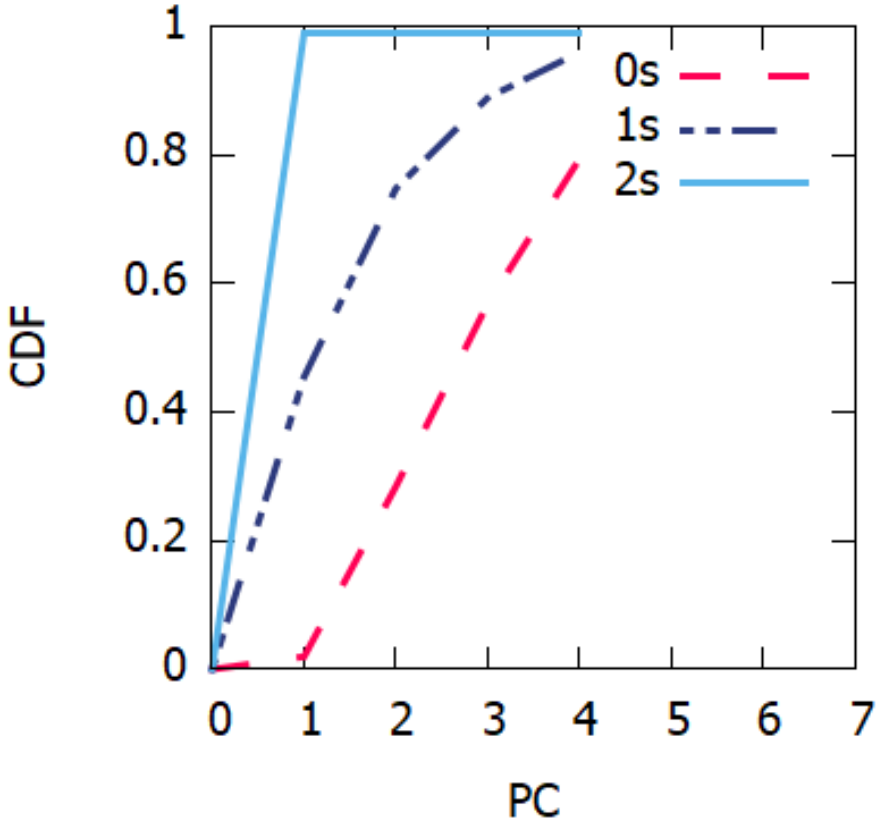

Figure 6.32: CDF random grid scenario with different silent period duration (0,1,2 seconds)

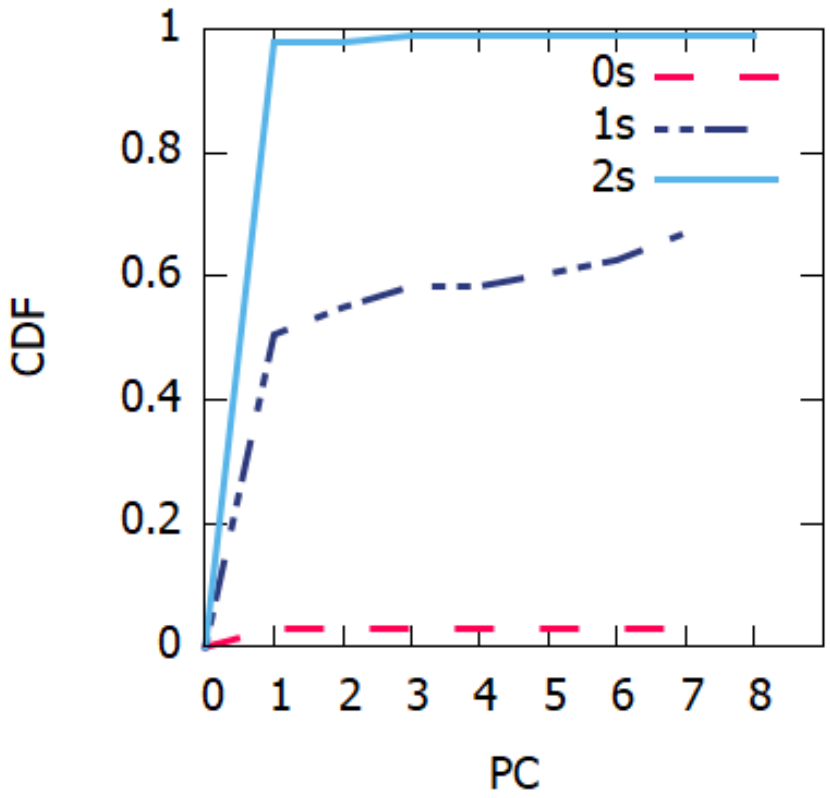

Figure 6.33: CDF random highway scenario with different silent period duration (0,1,2 seconds)

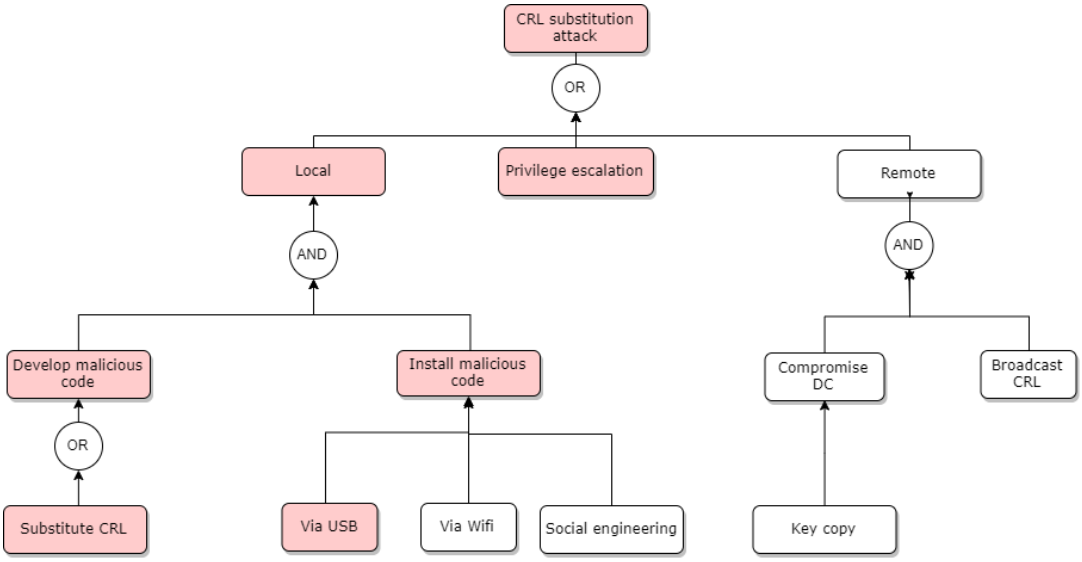

Figure 6.34: CRL substitution attack tree

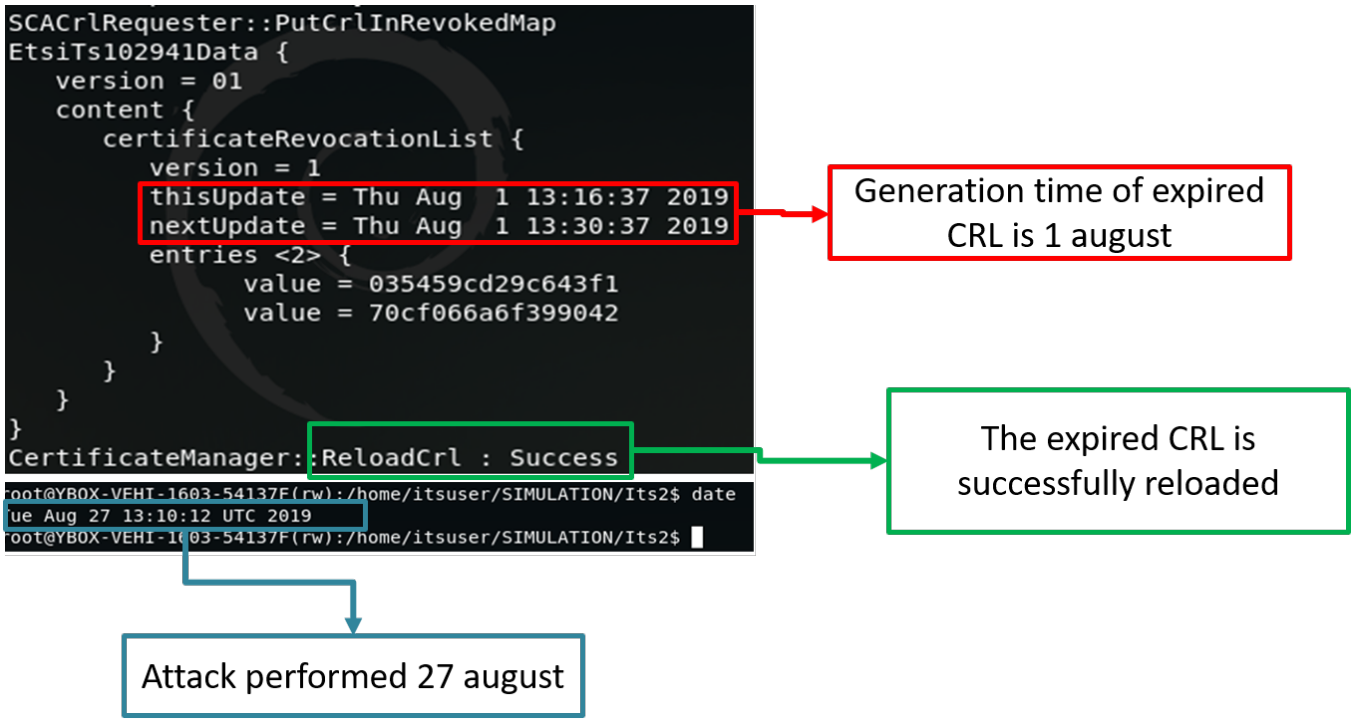

Figure 6.35: CRL substitution attack results

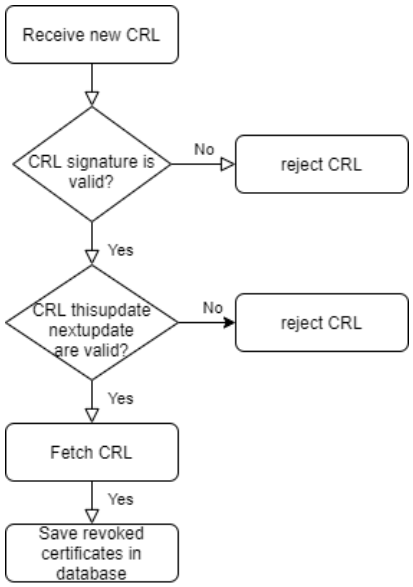

Figure 6.36: CRL verification algorithm

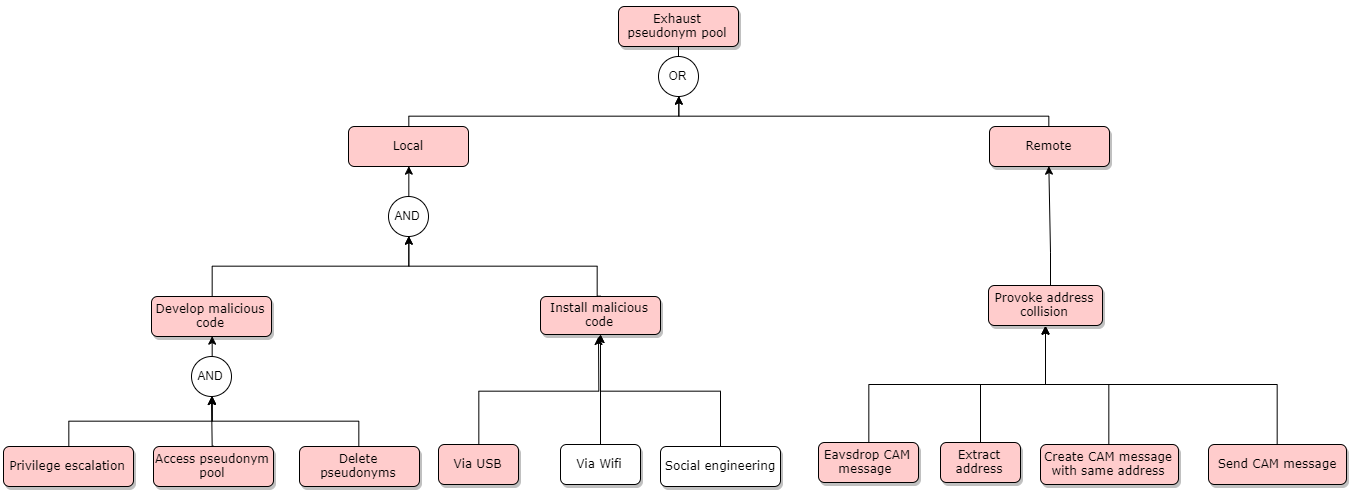

Figure 6.37: Exhaust pseudonym pool attack tree

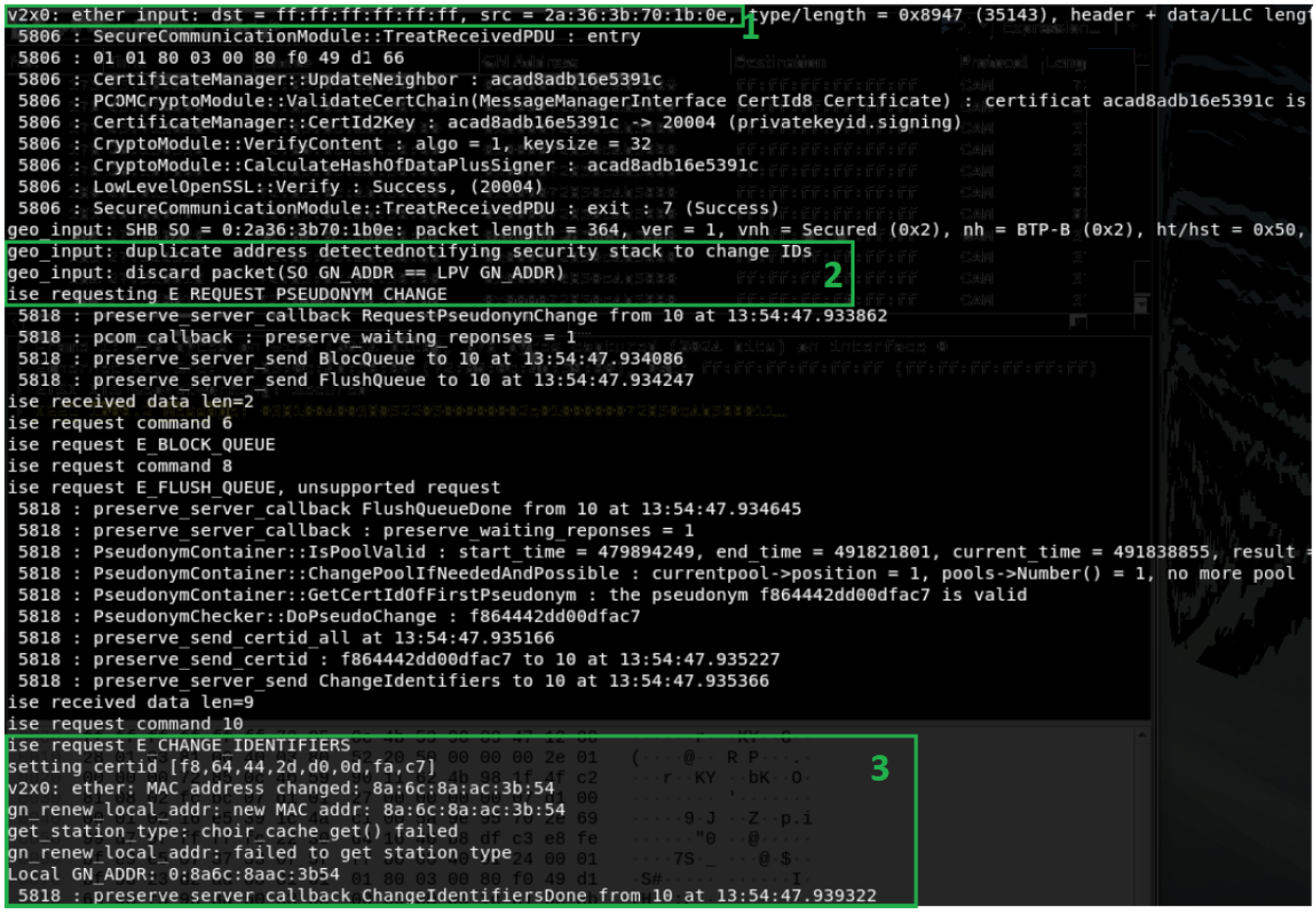

Figure 6.38: EPP attack

	Time	Source	GN Address	Destination	Protocol	Length	stationID
146	21.126919	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
149	21.530555	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	338	4176923011
152	21.939633	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
154	22.341715	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
157	22.755884	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	338	4176923011
160	23.170666	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
163	23.467866	2a:36:3b:70:1b:0e	0x00002a363b701b0e	ff:ff:ff:ff:ff:ff	CAM	378	2135766879
164	23.591640	8a:6c:8a:ac:3b:54	0x00008a6c8aac3b54	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
167	23.980331	8a:6c:8a:ac:3b:54	0x00008a6c8aac3b54	ff:ff:ff:ff:ff:ff	CAM	338	4176923011
170	24.383473	8a:6c:8a:ac:3b:54	0x00008a6c8aac3b54	ff:ff:ff:ff:ff:ff	CAM	335	4176923011
172	24.788633	8a:6c:8a:ac:3b:54	0x00008a6c8aac3b54	ff:ff:ff:ff:ff:ff	CAM	335	4176923011

Figure 6.39: Wireshark EPP

Chapter 7

Performance evaluation

Vehicles change frequently their pseudonym certificates. Which implies frequent reloading of pseudonym certificates from the PKI. Vehicles have a pool of multiple valid pseudonyms (a.ka Authorization ticket AT). When the pool is low on pseudonym certificates, vehicles triggers the pseudonym reload process.

This chapter presents the results of performance evaluation of the pseudonym reload process. The evaluation is realized in two phases: 1) performance evaluation of pseudonym reloading on ITS-G5 network and 2) on cellular network. For the ITS-G5 evaluation, we did on-table test and then in real environment while driving test. For cellular network evaluation, we did test for stopped vehicle and another test while driving.

The main objective of this evaluation is to test if the synchronous pseudonym certificate reloading from the PKI is feasible in real time while driving and to present the evaluation of the End to End latency.

7.1 Evaluation of pseudonym reloading on ITS-G5

We used the ISE project architecture and pseudonym reloading protocol (compliant with ESTI standard) for the ITS-G5 test. The ISE PKI protocol is described bellow:

7.1.1 ISE PKI protocols

The deployment of a new ITS-S follows the steps below:

1. **ITS-S registration**: the operator registers the new ITS-S to the EA. This operation is usually done using a secured web interface.

2. **Enrollment Certificate (EC) request**: the enrollment certificate request is presented in the left part of Figure 7.1. The registered ITS-S sends a request to the enrollment authority in order to get its EC. This operation can either be done directly by the operator or by the end user who purchased the ITS-S. As EC are long term certificates, an ITS-S usually requests one EC valid for a long period (several years).

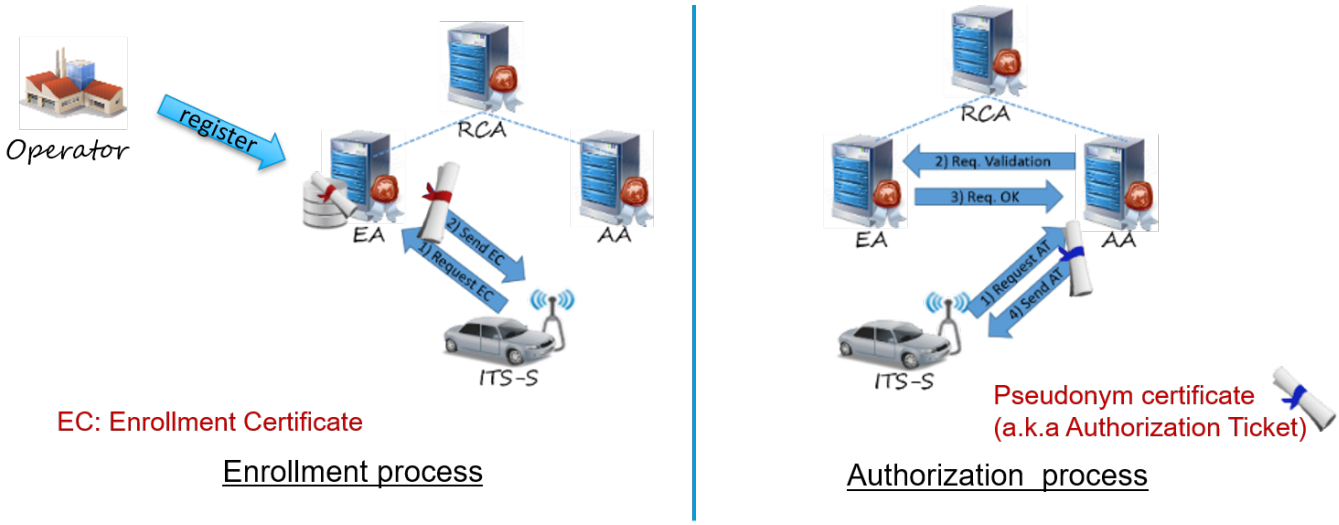

Figure 7.1: Enrollment and Authorization process

3. **Pseudonym certificate (PC) request**: The pseudonym certificate request is presented in the right part of Figure 7.1. The ITS-S sends pseudonym requests to the authorization authority in order to get a new PC. Before providing PC, the AA forwards the request to the EA. The EA verifies that the requesting ITS-S is legitimate and authorized to request PC. Depending on the response from the EA, the AA delivers or not new AT to the requesting ITS-S.

All the communication between the ITS-S and the PKI are done using HTTP.

7.1.2 Communication profiles for PKI requests

In order to send a PC request, vehicles can use one of the two communication profiles presented below:

- **TIG** (**T**CP/**I**Pv6/**G**5): the PC request is created and encapsulated in HTTP, TCP and IPv6. The request is then directly sent over the G5 network (802.11p).
- **TI3G** (**T**CP/**I**Pv6/**G**N6ASL/**G**N/**G**5): the PC request is created and encapsulated in HTTP, TCP and IPv6. It then goes through the GN6ASL (GeoNetworking to IPv6 Adaptation Sub-Layer) [81] and GN layers. Finally, the request is then sent over the G5 network.

Figure 7.2 details the path followed by data when the ITS-S sends a PC request to the PKI.

- The *Cert Reload* application requests the creation of a PC request to the security layer.
- The security layer generates the request, adds the HTTP header and sends it to the networking and Transport layer.
- The request is encapsulated into TCP and IPv6 headers.
- According to the selected profile (TIG or TI3G), the request is either directly sent to the Access layer or sent to the GN6ASL for encapsulation in a GN packet.
- The GN packet is then sent to the security layer for signature.

- The security layer signs the GN packet and returns it.
- The signed GN packet is sent to the Access layer.
- Finally, the 802.11p frame is sent over the G5 network.

The PC response coming from the PKI follows the same steps but in reverse order.

The difference between both profiles is the security. TI3G profile provides security over the ITS-G5 network (AT request is signed) which is not the case for TIG profile.

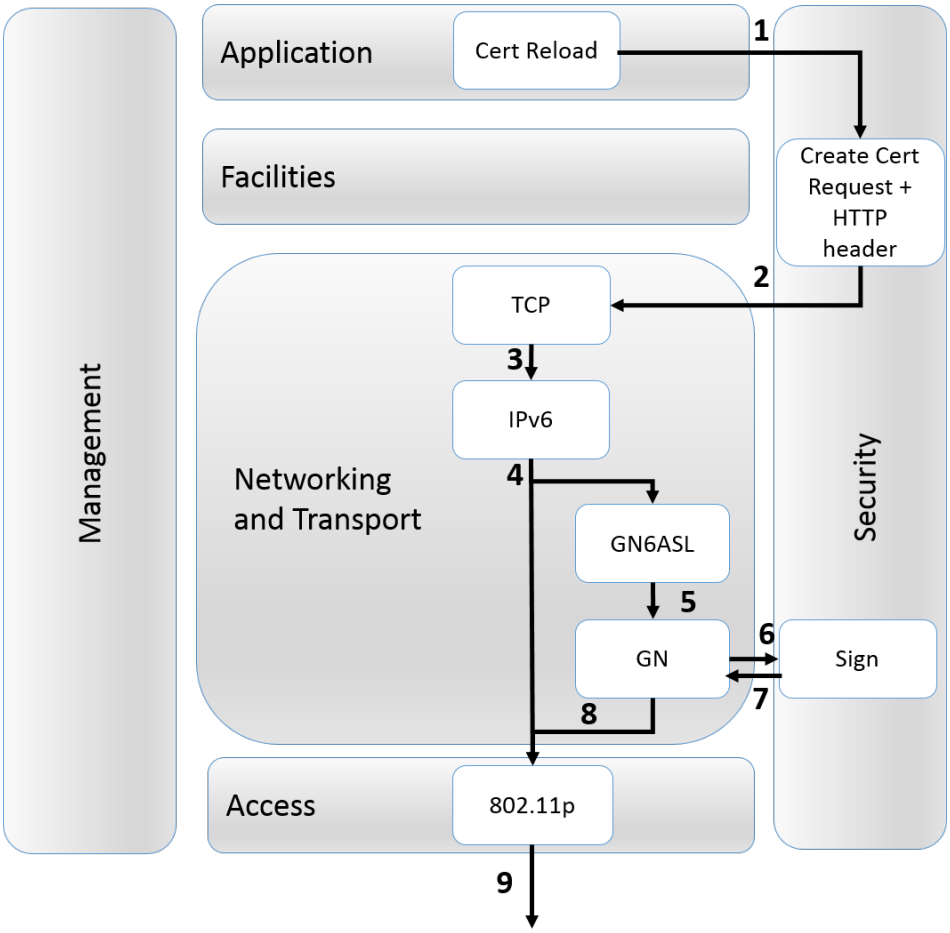

Figure 7.2: Data path within the ITS-S architecture when sending an AT request

7.1.2.1 Messages exchanges

Figure 7.3 is a sequence diagram showing the message exchange when the ITS-S requests pseudonyms using TIG or TI3G profile. The difference between both profiles is the computation and verification of geo-networking packet signatures at both OBU and RSU sides.

At the top of figure 7.3 we show the measured latencies:

- L_{ITS-S}: latency in the ITS-S. It consists of the creation of the request and the processing of the response. With the TI3G profile, it also includes the signature computation of the request and the signature verification of the response.

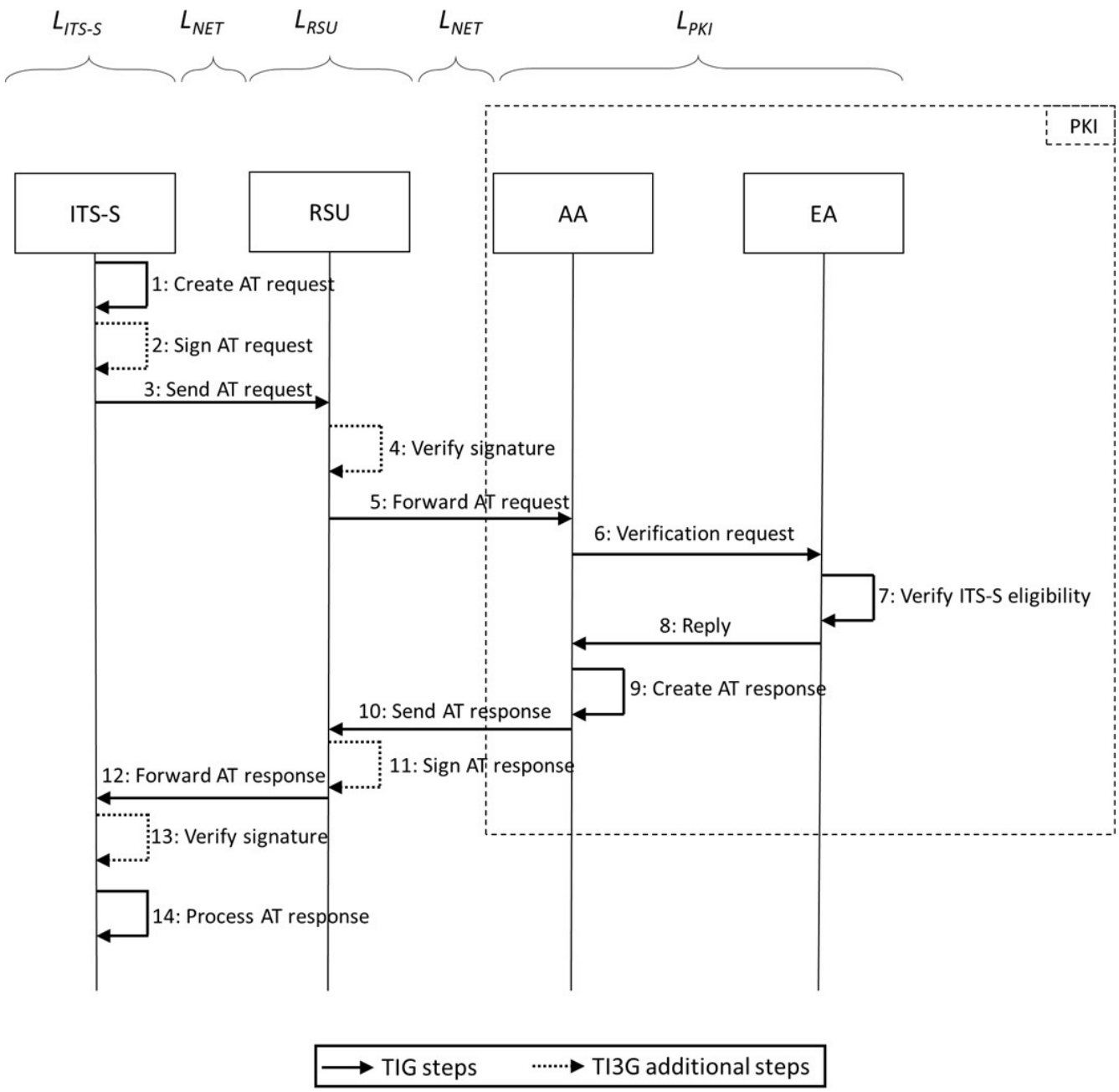

Figure 7.3: AT request/response using TIG or TI3G profile

- L_{NET}: latency of both G5 and Ethernet networks.
- L_{RSU}: latency in the RSU. It consists of the forwarding of both the request and the response between the two networks. With the TI3G profile, it also includes the signature verification of the request as well as the signature computation of the response.
- L_{PKI}: latency of the PKI. It consists of the verification of the request, its eligibility and the creation of the response.

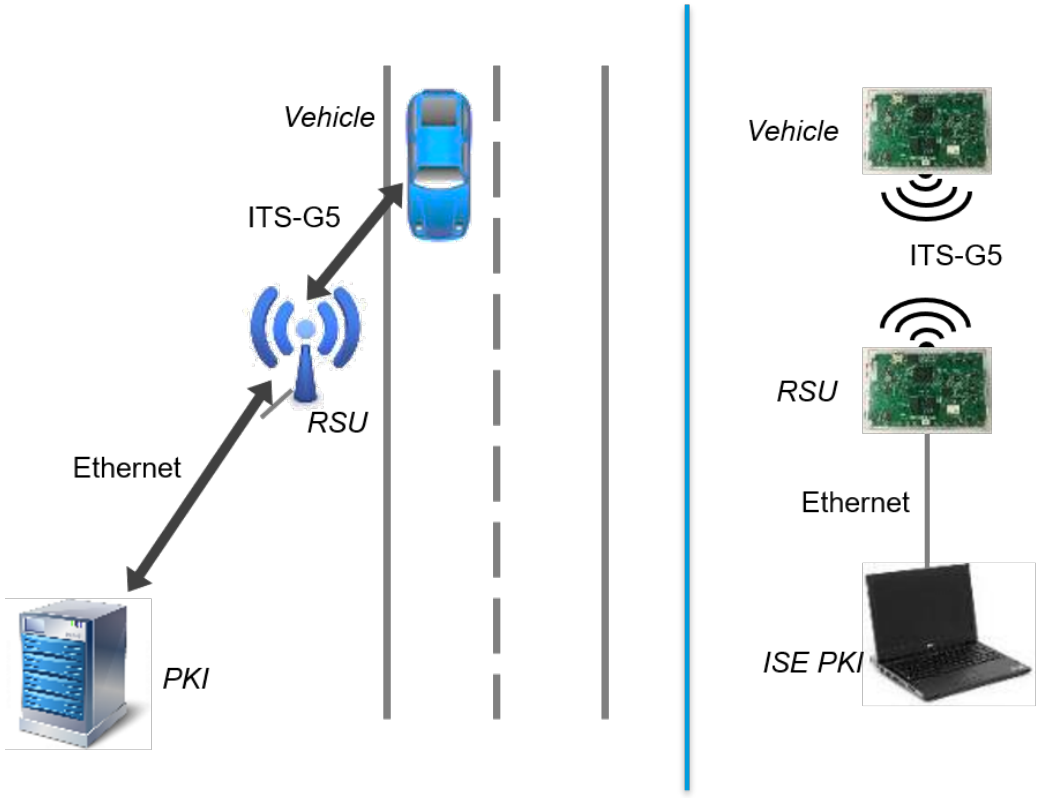

Figure 7.4: Use case picture (left) and testbed deployment (right)

7.1.3 Use case description

The use case is depicted on the left part of figure 7.4. A vehicle is within the range of the RSU that provides Internet access. The vehicles is low on pseudonyms and needs to refill its pool. It thus uses the RSU as a gateway forwarder to reach the PKI (located somewhere on the Internet) and requests new pseudonyms.

Note that the service advertisement (i.e. how the RSU advertises the vehicle that it provides Internet connectivity) as well as the vehicle IPv6 auto-configuration are not considered in this work.

7.1.4 On table evaluation

7.1.4.1 Testbed deployment

The testbed deployment of our experimentation is presented on the right of figure 7.4. We deploy two boards: one is the On-Board Unit (OBU) within the vehicle, and the other is the RSU. We deploy the PKI on a laptop. Table 7.1 summarizes the testbed specifications.

The OBU and the RSU are connected via the ITS-G5 network at 1-hop distance. As the PKI can be located anywhere on the Internet, it is difficult to estimate the connectivity between the RSU and the PKI. To lower the impact of the network latency between the RSU and the PKI as much as possible, we connected the two entities directly using a Gigabit Ethernet cable.

Before starting our experiments, we registered both OBU and RSU to the PKI and got their respective

Equipment	V2X Board	Laptop
Vendor	Renesas	Dell
Type	R-Car E2 Hideyoshi board	Latitude 3330
Architecture	ARMv7a	x86
OS	Linux Poky (Yocto project)	Linux Ubuntu 14.04 LTS
Connectivity	802.11p, GNSS, Ethernet	Ethernet
V2X software	ETSI V2X communication and security stacks	ISE PKI

Table 7.1: Specifications of the testbed equipment

EC by executing steps 1) and 2) of section 7.1.1.

For cryptographic operations, we use the well-known OpenSSL library.

7.1.4.2 Results and analysis

We conduct our experiments as follow: for each profile, the ITS-S sends one AT request to the PKI via the RSU. Once the pseudonym response is received, the ITS-S sends another request, and so on until reaching 1000 requests/responses.

- Packets size: Figure 7.5 shows the median packet size of a pseudonym request and response on the ITS-G5 network for both profiles. As we can observe, the packet size OF the TI3G profile is larger than the size for the TIG profile. This difference is due to the overhead generated by the geonetworking protocol and the Security stack: the geonet header + the security header + the signature.

- Latency: Figure 7.6 depicts the cumulative distribution function (CDF) of the pseudonym request/response round-trip latency for both profiles. We plot the horizontal line at 0.5 to show the median latencies: 440.051 ms for TIG profile and 728.657 ms for TI3G. The difference is explained by two reasons: 1) TI3G requires additional security operations (message signature/verification) and 2) TI3G packets size are larger, thus requires more time to be sent over the ITS-G5 network. Let us have a look at the round-trip latency in more details (remember it consists of L_{ITS-S} + L_{NET} + L_{RSU} + L_{PKI}). Figure 7.7 shows the distribution of each of these latencies (the median values are represented). With TI3G profile, we observe an increase in L_{ITS-S} and L_{RSU} due to the signature/verification operations (note that L_{RSU} is negligible with TIG profile as the RSU just forwards the packets), as well as, an increase in L_{NET} due to the extra time required to send larger packets over the network. L_{PKI} is not affected by the use of one or the other profile, thus it remains of the same order.

We also observe that L_{ITS-S} has the highest impact on the round-trip latency. Let us have a deeper look at this latency.

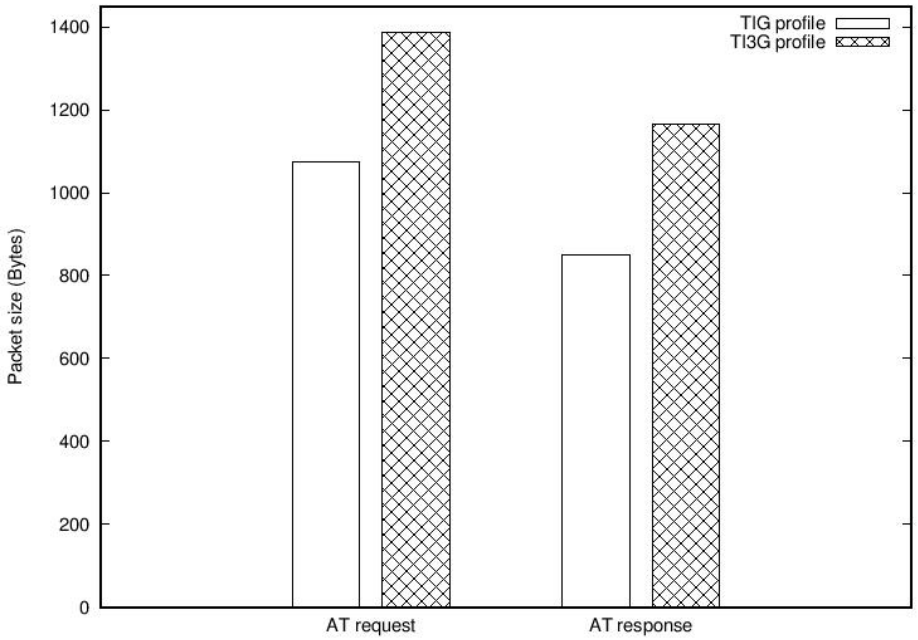

Figure 7.5: AT request/response median packet size on the G5 network

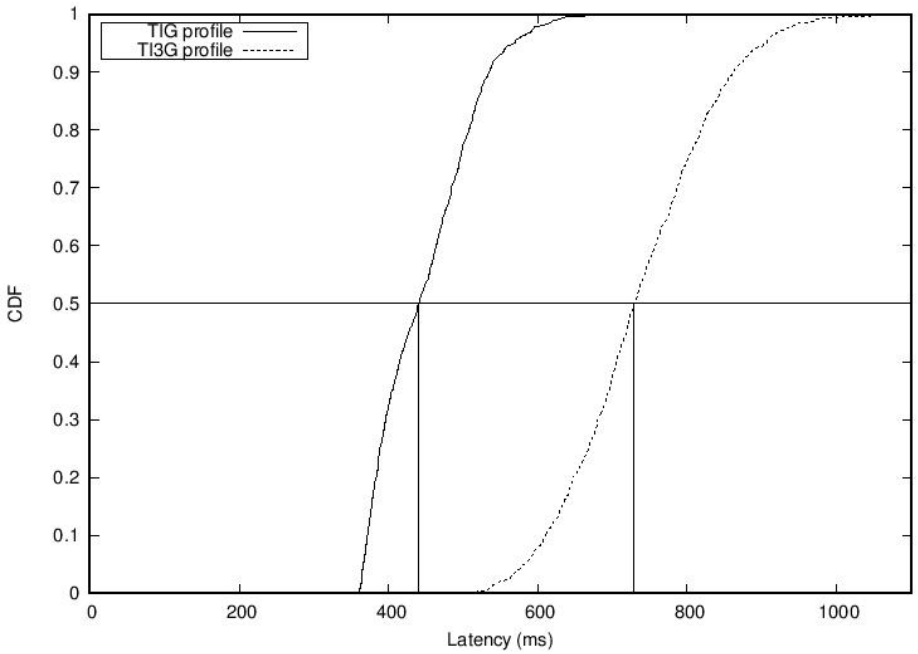

Figure 7.6: AT request/response round-trip latency

Figure 7.8 details L_{ITS-S}. We clearly observe that the AT request creation costs the most of the time. This is because it consists of 7 cryptographic operations: 3 for the generation of keys, 1 for HMAC, 1 for signature and 2 for encryptions.

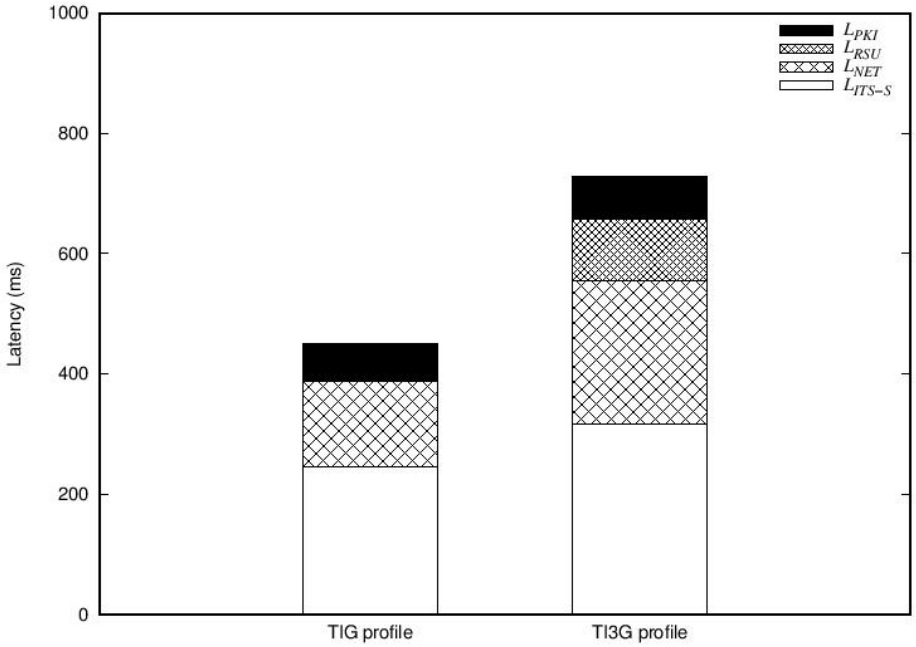

Figure 7.7: AT request/response detailed latency

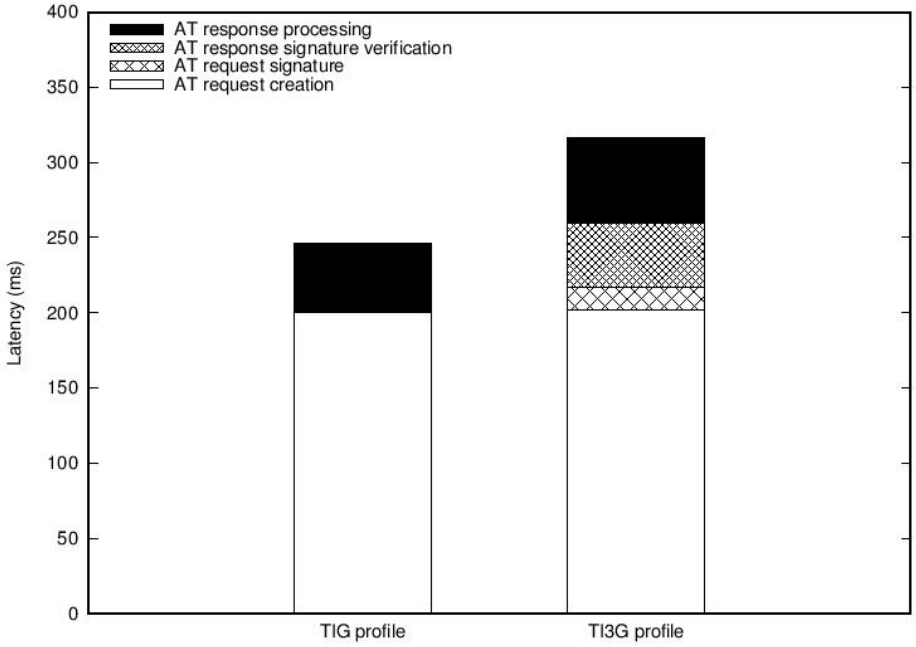

Figure 7.8: AT request/response detailed L_{ITS-S}

7.1.4.3 Discussion

The obtained results show that requesting an AT to the PKI requires about half a second, and even more in the case of a secured G5 communication (TI3G). Remember that our experiments are run in optimal conditions: the latency between the RSU and the PKI is negligible (direct connection via Ethernet) and the ITS-G5 network is not loaded (OBU and RSU are broadcasting only V2X messages). Therefore, the

round-trip latency in a real situation will be even higher.

Results also show that a lot of time is spent in cryptographic operations. This is quite interesting because optimizing such operations is feasible compared to reducing network latencies. For instance, integrating specific Hardware Security Modules (HSM) dedicated to cryptographic acceleration in ITS-S leads to lower round-trip latency.

7.1.5 In real environment evaluation

The considered use case is depicted in figure 7.4. A vehicle is within the range of the RSU that provides Internet access. The vehicle has a very few pseudonyms and needs to refill its pool. We evaluate the number of pseudonyms reloaded at the following speeds (km/h): 30, 50, 70 and 90. The ”in-RSU-range” detection mechanism works as follow: the vehicle sends ICMPv6 Echo Requests (or ”ping”) to the PKI. When the vehicle enters the range of the RSU, it receives back an ICMPv6 Echo Reply from the PKI. This response indicates that the vehicle can communicate with the PKI through the RSU. The vehicle then starts requesting new pseudonyms. When the vehicle moves out of the RSU's range (i.e. when no more new pseudonyms are received), the request of new pseudonyms is stopped. We configured the vehicle in such a way that it continuously requests new pseudonyms as long as it is within the RSU's radio coverage.

7.1.5.1 Test environment

The experimentations were conducted on the test track Val d or located at Versailles Satory (France) and using our prototype vehicle. The vehicle is provided by RENAULT and the model is a MEGANE COUPE as shown in figure 7.9. Figure 7.10 depicts a satellite view of the test track. We equipped the test track with one RSU represented by the red antenna. The green line shows the radio coverage of the RSU (about 940 meters), whereas the red line shows the road segment which is out of the coverage of the RSU. We equipped our prototype vehicle with an on-board unit (OBU), a Samsung tablet, a Raspberry Pi that provides an in-vehicle Wi-Fi access point (to connect the tablet with the OBU), and two IEEE 802.11p antennas that we placed on the vehicle's roof. The list of hardwares/softwares and the configuration of the antennas are presented in table 7.2.

7.1.5.2 Results and analysis

We run the experimentations as follows: we did two track laps for each speed (30, 50, 70 and 90 km/h) and for each communication profile (TIG and TI3G), resulting in a total of 16 laps. The main objectives of these experimentations are 1) to demonstrate the correct behavior of the system in a realistic environment and 2) to evaluate the system performance in terms of number of pseudonyms reloaded and the end-to-end latency.

- **Number of pseudonyms reloaded**: Figure 7.11 shows the number of successfully reloaded pseudonyms from the PKI versus the speed of the vehicle. The presented values are the sum of the two laps for each speed. We first observe that the number of successfully reloaded pseudonyms decreases as speed increases, following an exponential shape. This result was expected: the faster the vehicle moves, the less time it remains under the RSU radio coverage, thus the less time it has to reload

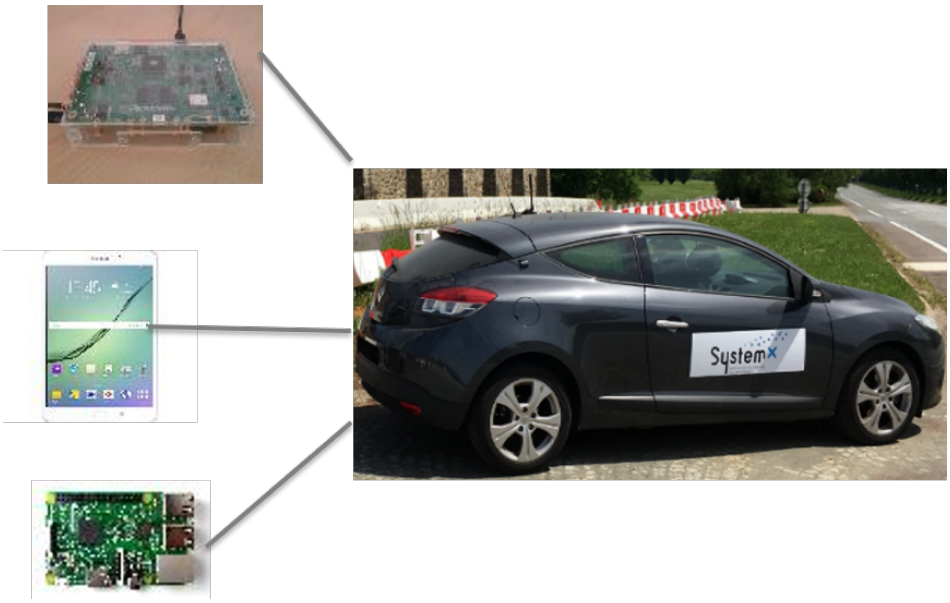

Figure 7.9: In-vehicle equipments

Figure 7.10: Google Maps ©: Versailles-Satory test track (green line = RSU coverage)

new pseudonyms. Second, we also observe that both curves have the same shape and the gap between them remains constant when speed increases. The gap is explained by the additional security processing required by the TI3G profile. Apart from the gap, the similar shape of both curves shows that the speed has the same impact on the performance, no matter what communication profile is used.

- **End-to-end latency**: Figure 7.12 depicts the median end-to-end latency of the pseudonym request/response for both profiles versus speed. We observe that the end-to-end latency is always shorter when using TIG profile. This was also observed during our in-lab experimentations and

OBU	Hardware	RENESAS R-Car E2 board
		Antenna with gain +9dBi
	Software	IEEE 802.11p driver
		V2X communication stack
		V2X security stack
		Pseudonym reloading application
RSU	Hardware	RENESAS R-Car E2 board
		Antenna with gain +6dBi
	Software	IEEE 802.11p driver
		V2X communication stack
		V2X security stack
PKI	Hardware	DELL Latitude 3330
	Software	ISE PKI
Config	ITS G5 channel	CCH(180)
	OBU radio power (incl. antenna gain)	+33 dBm e.i.r.p
	RSU radio power (incl. antenna gain)	+33 dBm e.i.r.p
	RSU radio coverage	940 meters

Table 7.2: Hardware and software configurations

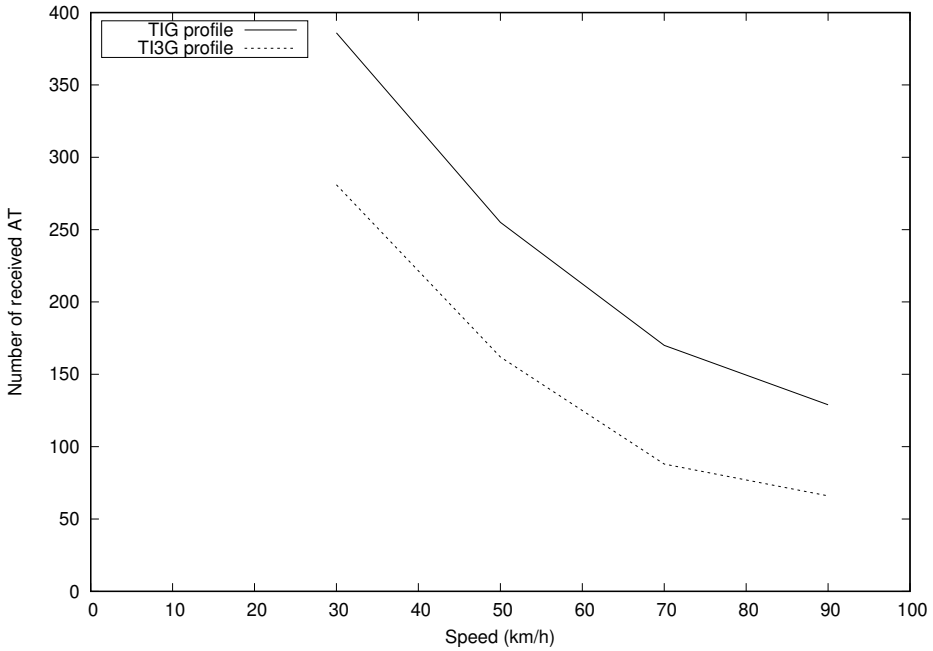

Figure 7.11: Number of pseudonyms (or AT) reloaded versus speed for both communication profiles

is explained by the additional security processing required by the TI3G profile. Also, the median end-to-end values remain roughly constant versus speed, i.e. the speed has no impact on the time required to successfully reload a pseudonym. Finally, the median end-to-end latency is roughly half a second to reload one pseudonym, which is quite high, especially for a highly mobile network.

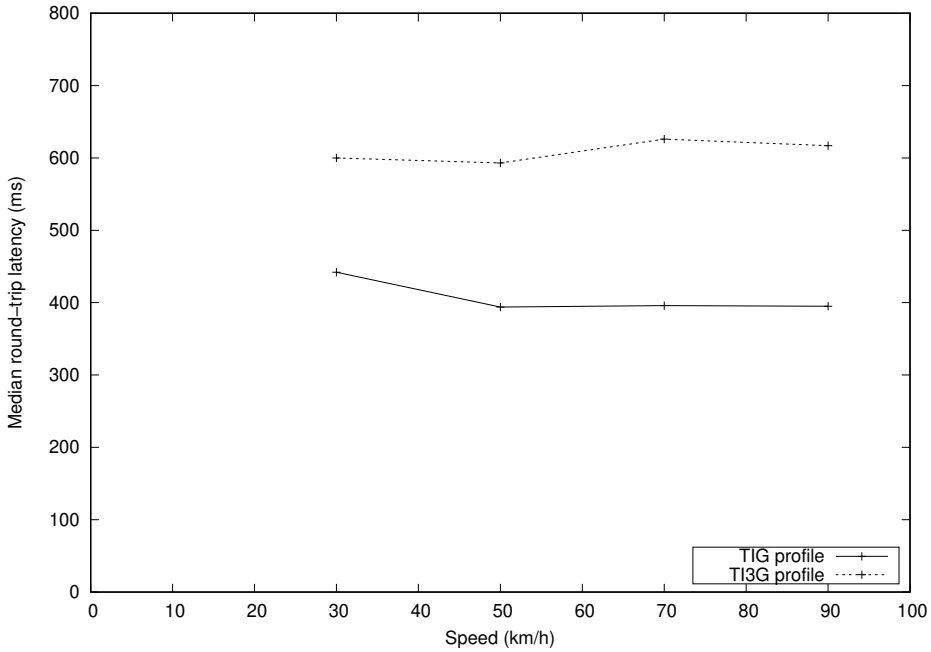

Figure 7.12: Pseudonyms reload median end-to-end latency versus speed

7.2 Performance Evaluation of pseudonym Reload over Cellular Technology

We used the SCOOP project architecture and pseudonym reloading protocol for the cellular test. The SCOOP onboad and offboard architecture is described bellow:

7.2.1 SCOOP onboard and offboard architecture

Figure 7.13 presents the in-vehicle components and the off-board architecture: Onboard components are:

- V2X module (VXU): this module contains the V2X communication stack, the security stack and the HSM. It is responsible of the AT request generation and the processing of AT response. It integrates a GPS module
- Telematic Control Unit (TCU): this module contains the SIM card responsible for all the cellular communication of the vehicle (i.e. it establishes the connection with the PKI server in case of AT request. The response pass through this module before being forwarded to the VXU.
- Head Unit (HU): this module controls the communication between the VXU and the TCU. It is also responsible for the IHM functions of SCOOP.
- GNSS antenna: located on the top of the vehicle to determine the vehicle's GPS position.
- ITS-G5 antenna: located on the top of the vehicle. It is responsible for the ITS-G5 communications (V2X message exchange).

Off-board components are:

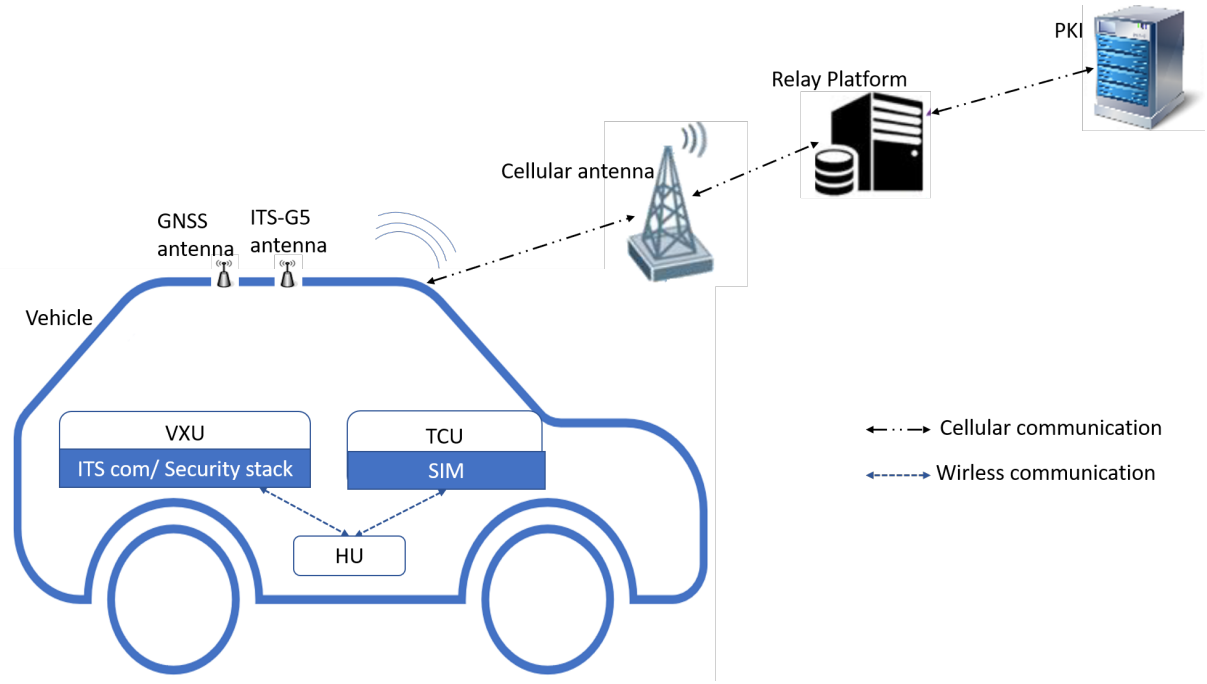

Figure 7.13: SCOOP onboard and offboard architecture

- Relay platform: this server is responsible for the forwarding of requests from the vehicle to the PKI and forwarding responses from the PKI to the vehicle. It authenticates the vehicles before forwarding requests.

- PKI: the PKI used in SCOOP is similar to that used in SCA project with slight difference in the named entities and certificates.

7.2.2 SCOOP AT reload protocol

The AT reload is depicted in Figure 7.14. It is similar to the ISE protocol, the difference is that the request/ response goes through the relay platform. The latencies are described below:

- L_{ITS-S}: latency in the ITS-S. It consists of the creation request in the VXU, the sending of the request to TCU, the response reception and processing by the VXU. It also includes the signature computation and verification by the ITS-S.

- L_{Relay} latency for the authentication of the ITS-S originating the pseudonym request, the forwarding of the request to the PKI and the forwarding of the response to the ITS-S.

- L_{NET}: same as presented in section 5.1.2.1

- L_{PKI}: same as presented in section 5.1.2.1

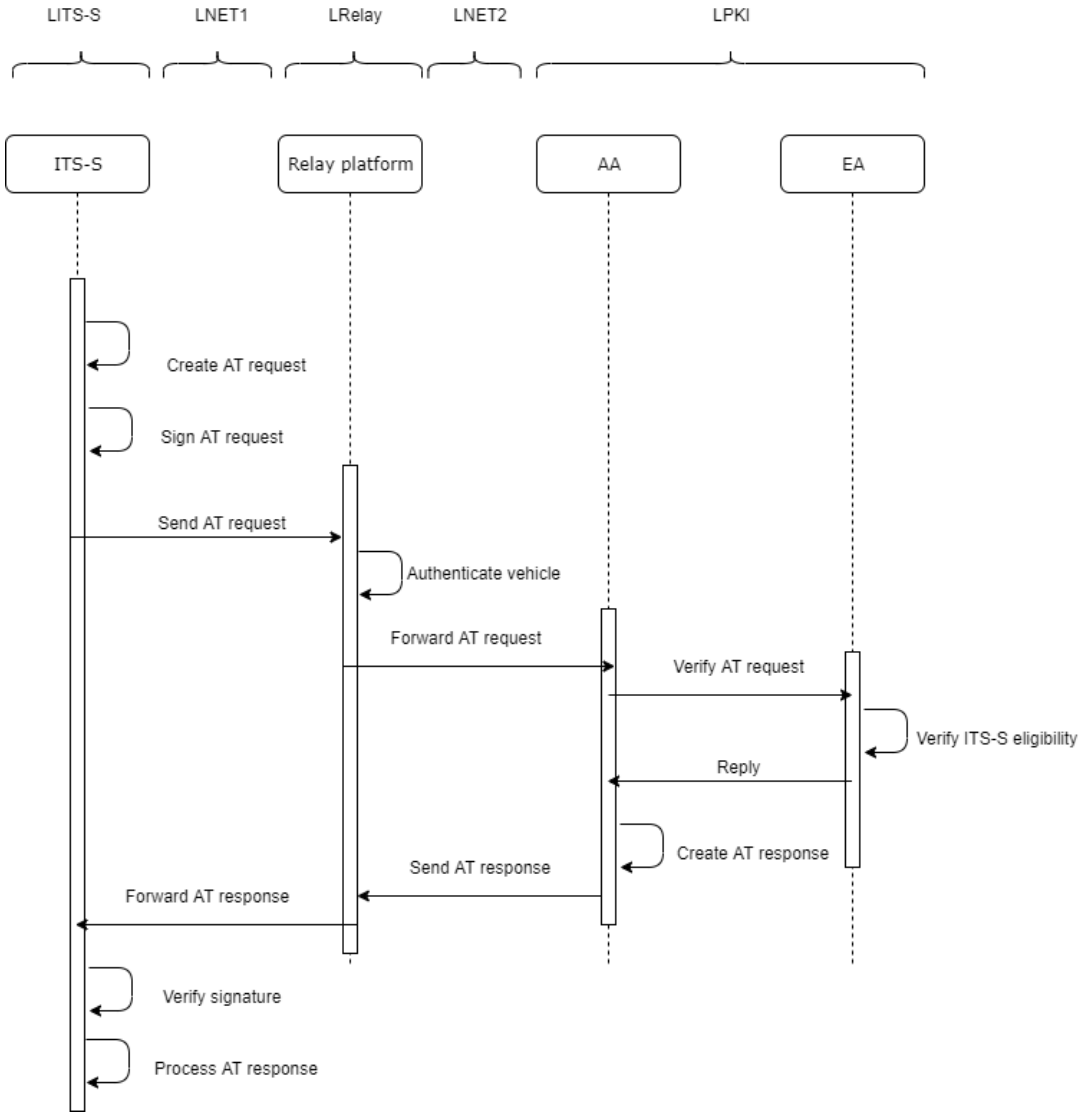

Figure 7.14: SCOOP AT reload protocol

7.2.3 Test environment

We conduct our experiments as follows: the ITS-S sends one AT request to the PKI following the protocol described before. Once the pseudonym response is received, the ITS-S sends another request, until reaching 400 requests/responses for stationary vehicle (static test) and 400 requests/responses for moving vehicle (dynamic test). The static test was performed in the parking of the Gradient building at Renault's Technocenter, and the dynamic test was run while driving from Renault's Technocenter to Versailles and vice versa. Figure 7.15 depicts a satellite view of the test place. The green line shows the route where the test was conducted. The used vehicle is provided by SCOOP RENAULT and the model is a MEGANE BERLINE as shown in figure 7.16.

7.2.4 Results

Performance measurements were done using 3G cellular network.

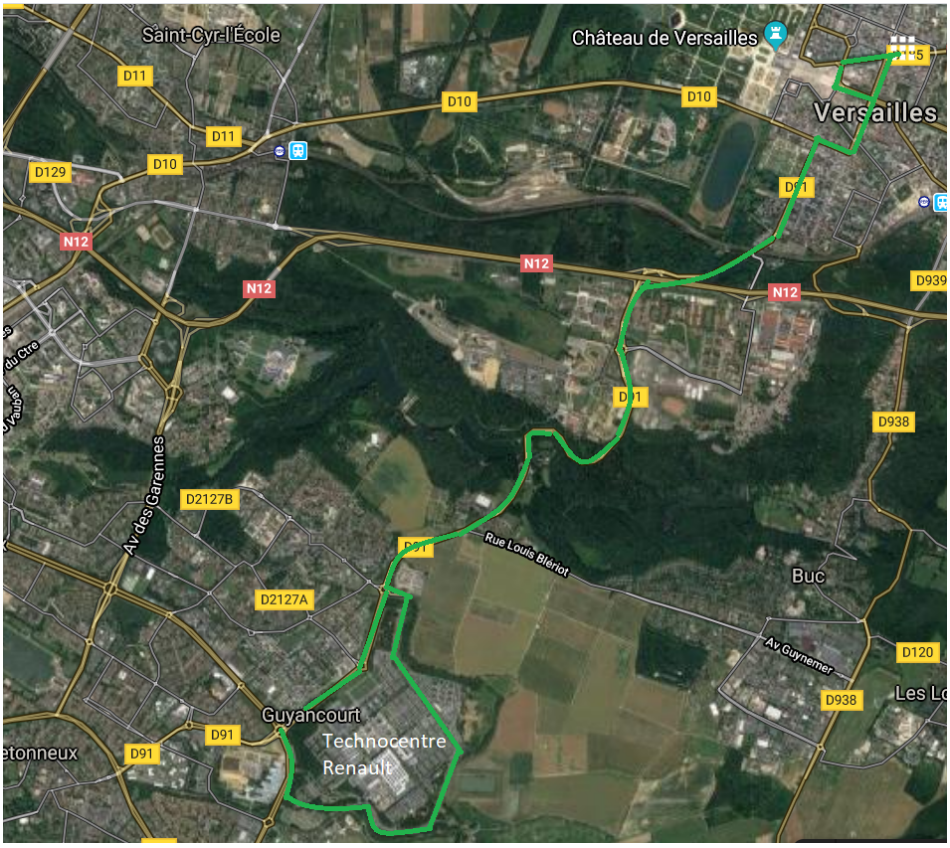

Figure 7.15: Google Maps ©: Open road (Technocentre Renault and Versailles route)- photo from google maps

Figure 7.16: SCOOP vehicle used in the test

- **Round trip end-to-end latency**: Figure 7.17 shows the cumulative distribution function (CDF) of the round-trip latency of AT request/response for a stopped and a moving vehicles. The horizontal

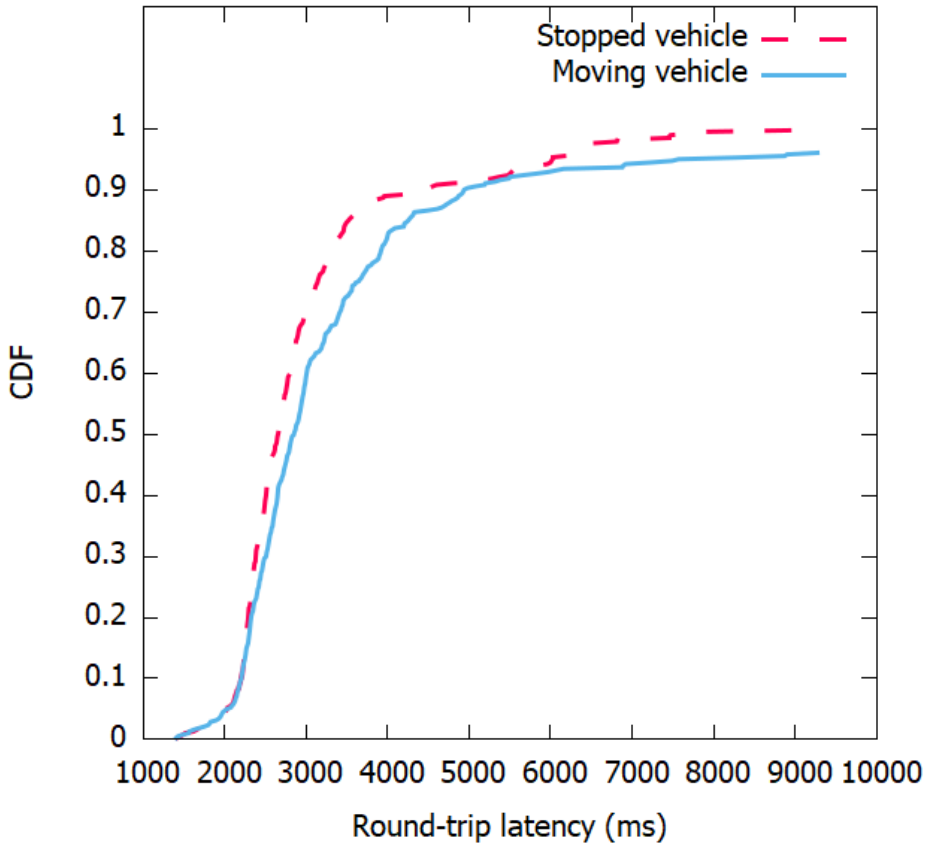

Figure 7.17: RTT AT request/response on cellular technology

line at 0.5 shows the median latencies: 2670 ms for a stopped vehicle and 2860 ms for a moving vehicle. The round-trip latency is the LITS + LNET+ LRelay+ LPKI. The interpretation of CDF if we take the point (2620, 0.3), it means that 30% of the requests/responses took 2620 ms or less. To find the percentage of requests/responses that took less than or equal to a defined latency, we can just find the y value corresponding to that latency using the graph of figure 7.17. The two curves (for stopped and moving vehicle) present the same curve shape.

- **Packet size**: Figure 7.18 shows the median packet size of a AT request and response on cellular network. As we can observe, the median packet size for the AT request is 920 bytes, for the AT response is 819 bytes and for the bas response (in case of AT request error) is 1528 bytes.

7.3 Conclusion

Vehicles need to reload frequently pseudonym certificate (a.k.a AT) from the PKI. In ISE and SCA project, they use the ITS-G5 technology to send the AT request via a RSU and receive the AT response. On the other hand, it is interesting to evaluate also the AT reloading on cellular technology. This is why, we used SCOOP project architecture and reload protocol to evaluate the AT reload on cellular.

In this chapter, we evaluated the performance of AT reloading on ITS-G5 and cellular technology. We focused on the round trip latency and the packet size on different technology and using different profiles

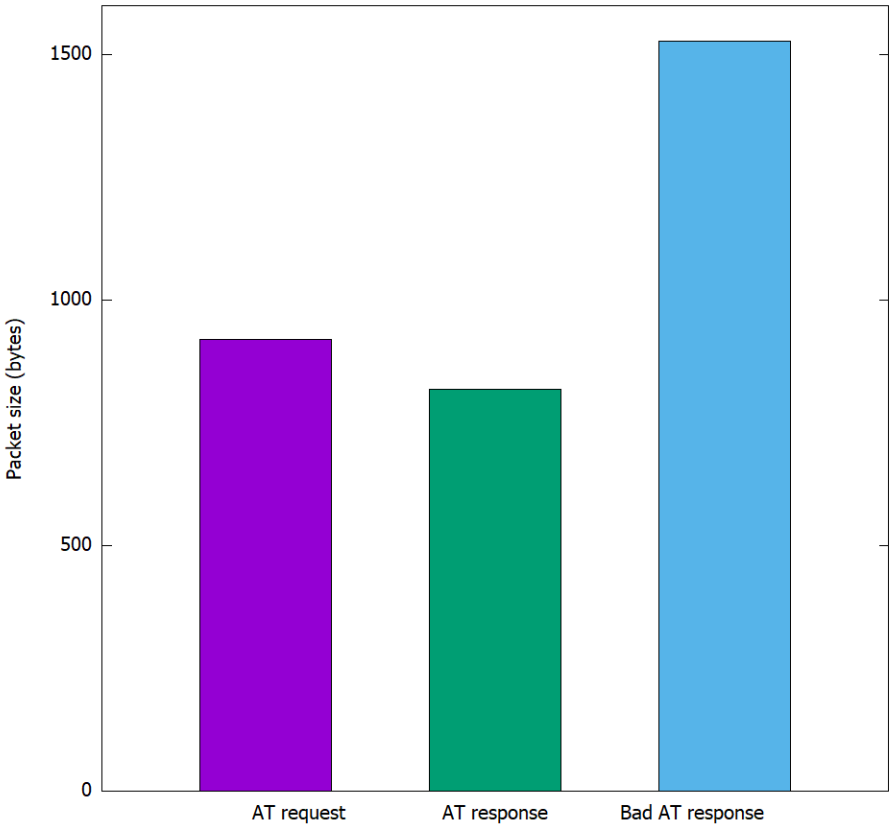

Figure 7.18: RTT AT request/response packet size on cellular technology

(with and without geo-networking). In the AT reload performance on ITS-G5, while driving, we evaluated also the number of AT reloaded when the vehicle passes in the range of the RSU. Results present that the velocity have an impact on the number of AT reloaded.

Chapter 8

Conclusion and perspectives

8.1 Summary

In this thesis, we started by investigating the state of the art in C-ITS: architecture, communication entities, message types, security and privacy issues and finally attacks on C-ITS.

We stated in chapter 2, the existing use cases in the literature. We concluded that applying any method such as risk analysis on those UC may be a long procedure. Thus, we proposed a classification methodology that analyze at first the security, privacy and technical requirements of each UC and classifies the UCs based on their requirements. The result of this analysis is the list of UCs that is used in this thesis. The selected use cases are: pseudonym reloading, pseudonym change, CRL/CTL distribution.

In chapter 3, we applied a risk analysis methodology (TVRA) on the selected UCs. Results of this risk analysis is a list of vulnerabilities and critical attacks that we must take into account.

In chapter 4, we implemented the critical attacks found in the risk analysis. We studied the feasibility of some attacks (Sybil, CRL substitution and exhaust of pseudonym pool) on real equipment. For Sybil attack we also proposed a detection mechanism based on reporting misbehavior vehicles to the MA located in the cloud. For the tracking attack, we evaluated a common pseudonym change strategy based on two attacker models (mid-sized and global attacker). For CRL substitution and exhaust of pseudonym pool, we proposed a methodology to deal with those attacks.

In chapter 5, we talked the problematic of reloading pseudonym certificates from the PKI in synchronous way. We evaluated the performance of pseudonym reloading in different context (using ITS-G5 and cellular network.

8.2 Perspectives

In this thesis, we studied security and privacy aspects in C-ITS focusing on ITS-G5 technology. Following the results obtained in chapter 4, we propose the investigation of security and privacy over cellular communication. Some of our selected use cases in chapter 2 (HD Map, high density platooning) need cellular network as well as many other investigation on future use cases such UC related to fully autonomous driving. It would be interesting to continue this work on these UCs.

Another perspective is the choice of technology per UC and the resilience of technology for autonomous vehicles. Current ETSI standards handle only the ITS-G5 part, many security use cases may be better handled using cellular technologies. It may be important to study the choice of technology depending on UC analysis.

Chapter 9

List of publication

Conference papers:

- Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN, Richard DENIS, C-ITS use cases: study, extension and classification methodology, *IEEE 87th Vehicular Technology Conference (VTC), 2017, Porto – Portugal*.
- Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN, Risk Analysis on C-ITS pseudonymity aspects, *IEEE/IFIP 10th New Technologies, Mobility and Security (NTMS), 2019, Canary island – Gran canaria*.
- Joseph KAMEL,Farah HAIDAR, Ines BEN JEMAA, Arnaud KAISER, Brigitte LONC, Pascal URIEN, A Misbehavior Authority System for Sybil AttackDetection in C-ITS, *10th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communication Conference (UEMCON), 2019, New York – USA*
- Farah HAIDAR, Arnaud KAISER, Brigitte LONC, On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security, *IEEE 86th Vehicular Technology Conference (VTC), 2017, Toronto – Canada*
- Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN, C-ITS PKI protocol: Performance Evaluation in a Real Environment, *IEEE/IFIP 15th Wireless On-demand Network systems and Services Conference (WONS), 2019, Wengen – Switzerland*
- Farah HAIDAR, Joseph KAMEL, Ines Ben Jemaa, Arnaud Kaiser, Brigitte LONC, Pascal Urien, DARE dataset specifications for each scenario, *IEEE 91th Vehicular Technology Conference (VTC), 2020, Antwerp – Belgium*
- Farah HAIDAR, Farah BRAITEH, Brigitte LONC, and Pascal URIEN ,Performance Evaluation of Pseudonym Reload overCellular Technology, *IEEE/IFIP 11th New Technologies, Mobility and Security (NTMS), 2021,paris* (Submitted)

Journal

- Brigitte LONC, Farah HAIDAR, Denis FILATOV, Cooperative ITS Security Standards: Implementation, assessment and next challenges, *the 14th ITS European Congress, 18-20 May 2020, Lisbon – Portugal*

APP

- Tracker Farah: App on tracking attack
- SAC: App on Sybil attack

Chapter 10

Annex 1

10.1 TVRA method tables

This section presents the tables used in the TVRA method.

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context	3

Table 10.1: Asset impact

Vulnerability rating	Threat-level				
	Negligible	Low	Moderate	Severe	Critical
Basic	Possible	Likely	Very Likely	Very Likely	Very Likely
Enhanced	Basic	Unlikely	Possible	Likely Very Likely	Very Likely
Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
Beyond High	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

Table 10.2: Mapping of vulnerability rating with Threat level to identify likelihood of attack

10.2 Embedded Architecture for ITS-S

Protection of V2X communication and internal data in C-ITS is paramount. Most relevant threats described in the risk analysis of this thesis are considered to define a proper architecture regarding its impact on C-ITS system. Many works on security architecture were done by moalla et al. [82] and in many projects such as PRESERVE . In this Annex, we propose an embedded architecture, presented in Figure 10.1,

Factor	Range	Value
Time	≤ 1 day	0
	≤ $1week$	1
	≤ $2week$	2
	≤ $1month$	4
	≤ $2months$	7
	≤ $3months$	10
	≤ $4months$	13
	≤ $5months$	15
	≤ $6months$	17
	> $6months$	19
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Opportunity	Unnecessary/unlimited access	0
	Easy	1
	Moderate	4
	Difficult	10
	None	999
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

Table 10.3: Factor and values

that aims at preventing of some threats tested in this thesis. This can be as recommendations that can be integrated in further works in the global ITS-S architecture.

- System Information Module (SIM): is responsible for communication of some information related to system such as engine status (active or not), distance traveled since last engine activation, sensor and GPS information etc...
- Secure Communication Module (SCM): is the access point between SIM and internal modules such as PMM, CSM etc...
- Misbehavior Detection Module (MDM): is responsible for the consistency and plausibility checks, thus the local detection of misbehaving entity. It is also responsible for sending misbehavior report to the MA.
- Pseudonym Management Module (PMM): is responsible for the management of vehicle's pseudonym pool such as pseudonym change.

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of
0 to 9	Basic	No rating
10 to 13	Enhanced-basic	Basic
14 to 19	Moderate Enhanced	basic
20 to 24	High	Moderate
> 24	Beyond High	High

Table 10.4: Attack potential

Value	Risk
1,2	Minor
3,4	Major
6,9	Critical

Table 10.5: Risk

- Logs Module (LM): is responsible for logging information that can be important in case of system problem or failure.
- ID Management Module (IDMM): is responsible for the management of the vehicle's identifiers, it triggers pseudonym and Enrollment certificate reloading from the PKI.
- Certificate Store Module (CSM): stores the pseudonym certificates. It is the pseudonym pool.
- Hardware security Module (HSM): is responsible for:
  - Secure Key Store Module (SKSM): the SKSM is responsible for storing secret keys.
  - Cryptographic Services Module (CSM): the CSM is responsible for the of cryptographic operations such as encryption, signature, and signature verification etc...
  - Secure Store Module (SSM): the SSM stores some sensitive information such as CRL, and CTL.

Asset impact	Attack intensity	Resulting impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3
3	0	3
3	1	3
3	2	3

Table 10.6: Result on overall Impact of varying attack intensity

Attack intensity	Value
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

Table 10.7: Attack intensity levels

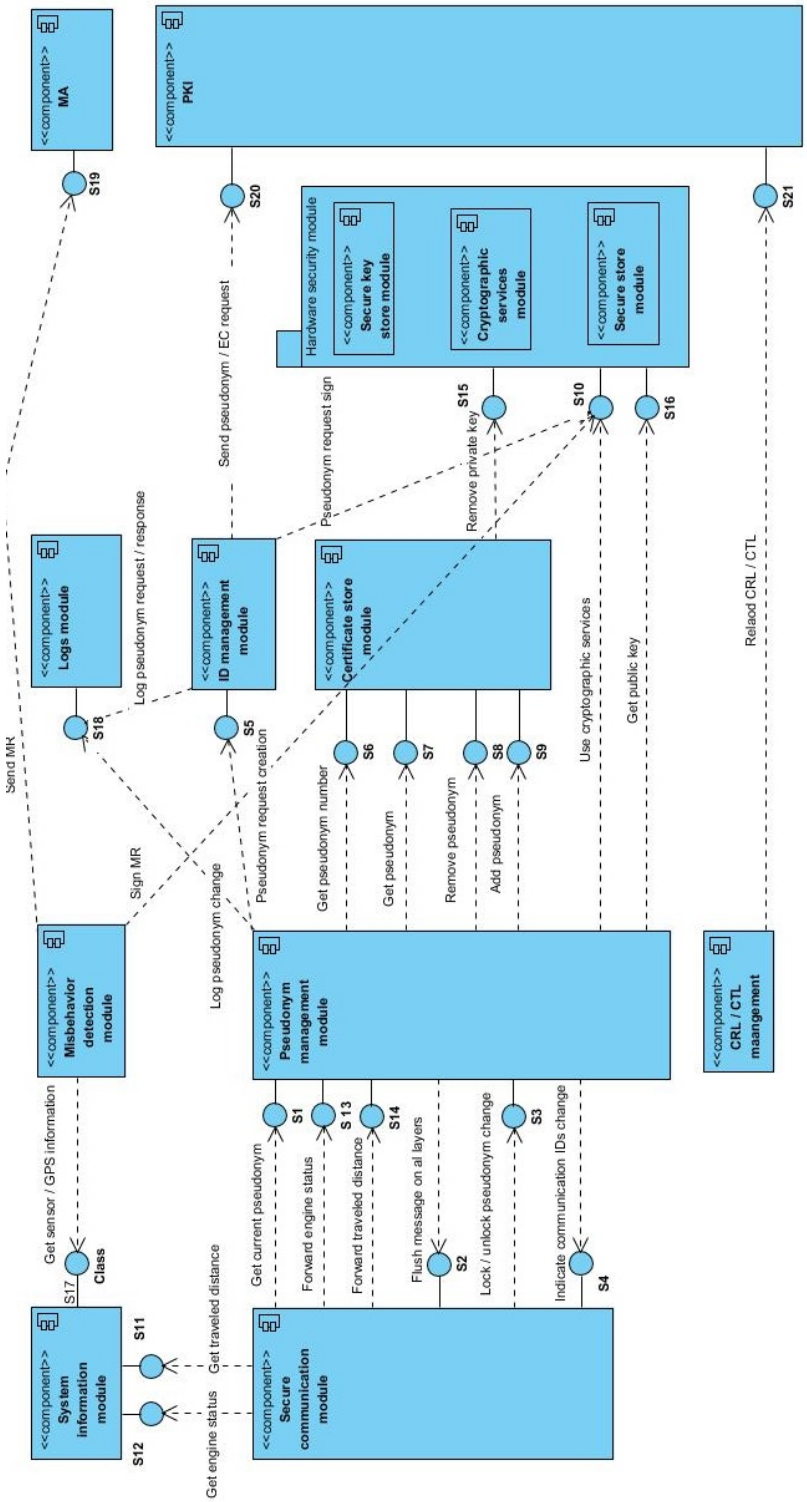

Figure 10.1: Embedded security architecture

Interface	Services
S1	SCM get current pseudonym certificate from the PMM
S2	In case of pseudonym change, the PMM may ask the SCM to remove all queued messages
S3	When an event is detected, the vehicle create and send a DENM to inform other vehicles about the situation. This interface permit to lock and unlock pseudonym change in such cases.
S4	In case of pseudonym change, the PMM communicate the new ID to the SCM through this interface
S5	When the certificate store is low in pseudonym (number of pseudonyms ¡ threshold), the PMM asks the IDMM to create a pseudonym request.
S6	To decide if the vehicle should reload pseudonym certificates, the PMM communicates through this interface with the CS to get the number of remaining pseudonyms
S7	PMM asks for a valid pseudonym from the CS
S8	Depending on the pseudonym change strategy, the PMM decides when the vehicle should stop using a pseudonym certificate and thus remove it from its CS
S9	After a successful pseudonym certificate reloading, the PMM stores the certificates in the CS
S10	The PMM, the MDM, and the ID management module can use the cryptographic services provided by the HSM. Services can be signature of pseudonym request, verification of signature etc..
S11	Some pseudonym change strategies are based on traveled distance. The SIM communicates traveled distance to the SCM that forwards it to the PMM
S12	Some pseudonym change strategy are based on engine status. The SIM communicate engine status to the SCM that forward it to the PMM
S13	Forwards engine status to the PMM
S14	Forwards traveled distance to the PMM
S15	PMM may ask the HSM to remove the private key corresponding to a removed public key
S16	PMM may ask the HSM to get the public key
S17	Embedded MDM requires information from SIM in order to detect misbehaving vehicles. Information can be sensor data, GPS or other.
S18	Logging different events is also important. PMM and IDMM log some events such as pseudonym change triggering, pseudonym reloading, etc...
S19	In case of local misbehavior detection. The MDM sends a Misbehavior report to the MA.
S20	IDMM sends pseudonym or EC request to the PKI

Table 10.8: Interfaces

Bibliography

[1] MohamedNidhalMejri, Jalel Ben-Othman, MohamedHamdi. Survey on VANET security challenges and possible cryptographic solutions. *ScienceDirect*, pages 53–66, May 2014.

[2] Kim-Kwang Raymond Choo Quang Do, Ben Martini. The Role of the Adversary Model in Applied Security Research. *Cryptology ePrint Archive*, March 2018.

[3] Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN, Richard DENIS. C-ITS use cases: study, extension and classification methodology. In *IEEE 87th Vehicular Technology Conference (VTC)*, 2017.

[4] Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN. Risk Analysis on C-ITS pseudonymity aspects. In *IEEE/IFIP 10th New Technologies, Mobility and Security (NTMS)*, 2019.

[5] Joseph KAMEL,Farah HAIDAR, Ines BEN JEMAA, Arnaud KAISER, Brigitte LONC, Pascal URIEN . A Misbehavior Authority System for Sybil AttackDetection in C-ITS. In *10th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communication Conference (UEMCON)*, 2019.

[6] Farah HAIDAR, Joseph KAMEL, Ines Ben Jemaa, Arnaud Kaiser, Brigitte LONC, Pascal Urien . DARE dataset specifications for each scenario. In *IEEE 91th Vehicular Technology Conference (VTC)*, 2020.

[7] Farah HAIDAR, Arnaud KAISER, Brigitte LONC. On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security. In *IEEE 86th Vehicular Technology Conference (VTC)*, 2017.

[8] Farah HAIDAR, Arnaud KAISER, Brigitte LONC, Pascal URIEN. C-ITS PKI protocol: Performance Evaluation in a Real Environment. In *IEEE/IFIP 15th Wireless On-demand Network systems and Services Conference (WONS)*, 2019.

[9] ETSI EN 302 663 V1.2.0. Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. 2012.

[10] Autotalks and al. ITS-G5 technology – A Fact Sheet. 2010.

[11] ETSI 302 637-2 V1.4.0. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. 2018.

[12] Hou Liping, Shi Lei. Research on Trust Model of PKI. *Fourth International Conference on Intelligent Computation Technology and Automation*, pages 232–235, 2011.

[13] ETSI TS 102 940 V1.3.1. Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. pages 338–350, 2018.

[14] William Whyte, Andre Weimerskirch, Virendra Kumar, Thorsten Hehn. A Security Credential Management System for V2V Communications. *IEEE Vehicular Networking Conference*, pages 22–23, 2013.

[15] Matthew D. Furtado ; Robert D. Mushrall ; Hong Liu. Threat Analysis of the Security Credential Management System for Vehicular Communications. *IEEE International Symposium on Technologies for Homeland Security (HST)*, 2018.

[16] David Cham, Eugtne van Heyst. Group Signatures. *EUROCRYPT '91*, pages 257–265, 1991.

[17] CAR 2 CAR Communication Consortium. https://www.car-2-car.org//.

[18] ETSI. EN. 302 665 V1.1.1. Intelligent Transport Systems (ITS); Communications Architecture. pages 13–16, September 2010.

[19] ISO/IEC 7498-1. Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model. 1994.

[20] EN 302 636-5-1 V1.2.1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol. 2014.

[21] EN 302 636-4-1 V1.2.1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independant Functionality. 2014.

[22] EN 302 636-6-1 V1.1.1. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols. 2011.

[23] ETSI TS 102 894-1. Intelligent Transport Systems (ITS); Users and applications requirements; Part 1: Facility layer structure, functional requirements and specifications. 2013.

[24] 1609.0-2013. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture. 2013.

[25] Meriem HOUMER, Moulay Lahcen HASNAOUI and Abdeslam ELFERGOUGUI. Security Analysis of Vehicular Ad-hoc Networks based on Attack Tree. *International Workshop on Technologies, Algorithms, Models, Platforms and Applications for Smart Cities*, 2018.

[26] Madhavi sinha Ankit Kumar. Overview on Vehicular Ad Hoc Network and its Security Issues. *2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018.

[27] Maxim Raya, Jean-Pierre Hubaux. Security aspects of inter-vehicle communications. *5th Swiss Transport Research Conference (STRC)*, 2005.

[28] Bryan Parno, Adrian Perrig. Challenges in Securing Vehicular Networks. *HotNets-IV*, 2005.

[29] R. Sures Ghassan Samara, Wafaa A.H. Al-Salihy. Some Properties of Uniform Step Size Quantizers. *Second International Conference on Network Applications, Protocols and Services*, 2010.

[30] Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Ju Bin Song, and Husheng Li. A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids. *IEEE TRANSACTIONS ON SMART GRID*, 6, 2015.

[31] Abdelwahab Boualouache, Sidi-Mohammed Senouci, Samira Moussaoui. A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks. In *IEEE Communications Surveys Tutorials*, 2017.

[32] Jonathan Petit,Djurrre Broekhuis, Michael Feiri, Frank Kargl. Connected Vehicles: Surveillance Threat and Mitigation. *Black Hat Europe*, 2015.

[33] ETSI TS 102 165-1 V5.2.3. CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA). 2017.

[34] ETSI TR 102 638 V1.1.1. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. 2009.

[35] Guillermo Pocovi, Mads Lauridsen, Beatriz Soret, Klaus I. Pedersen, Preben Mogensen. Automation for On-road Vehicles: Use Cases and Requirements for Radio Design. In *Vehicular Technology Conference (VTC Fall)*, 2015.

[36] 5GPPP. 5G Automotive Vision. In *5GPP white paper*, October 2015.

[37] Katrin Sjoberg, Peter andres, teodor Buburuzan, and achim Brakemeier. Cooperative Intelligent transport systems in europe Current Deployment Status and Outlook. In *Vehicular Technology Magazine*, June 2017.

[38] ETSI . ETSI TR 102 893, Intelligent Transport Systems (ITS) Security Threat Vulnerability and Risk Analysis (TVRA). 2017.

[39] Rim MOALLA, Brigitte LONC, Houda LABIOD, Noemie SIMONI. How to Secure ITS Applications? . In *Ad Hoc Networking Workshop (Med-Hoc-Net)*, June 2012.

[40] Kiri Wagstaff, Claire Cardie, Seth Rogers, and Stefan Schroedl. Constrained K-means Clustering with Background Knowledge. In *International Conference on Machine Learning*.

[41] K. A. Abdul Nazeer, M. P. Sebastian . Imroving the Accurancy and Efficiency of the K-means Clustering Algorithm. In *World Congress on Engineering*, 2009.

[42] Pradeep Kumar Singh. Clustering Techniques in Data Mining: A Comparison. *Bharati Vidyapeeth's Institute of Computers, Applications and Management (BVICAM)*, pages 170–182, 2015.

[43] Berrehili Fatima zahra, Belmekki Abdelhamid. Risk analysis in Internet of Things using EBIOS. In *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017.

[44] ETSI. ETSI TS 102 165, CYBER, Methods and protocols, Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) . 2017.

[45] Rim MOALLA, Houda LABIOD, Brigitte LONC, Noemie SIMONI. Risk Analysis Study of ITS Communication Architecture. In *Third International Conference on The Network of the Future (NOF)*, 2012.

[46] J. Douceur. the Sybil Attack. In *First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer*, 2003.

[47] Joseph Kamel, Arnaud Kaiser, Ines Ben Jemaa, Pierpaolo Cincilla, Pascal Urien. CaTch: A Confidence Range Tolerant Misbehavior Detection Approach. In *IEEE Wireless Communications and Networking Conference (WCNC)*, 2019.

[48] European Commission (EC). Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). *Cooperative, connected and automated mobility (CCAM)*, pages 1–36, December 2017.

[49] AA. Pouyan and M. Alimohammadi. Sybil Attack Detection in Vehicular Networks. In *Computer Science and Information Technology 2.4*, pages 197 – 202, 2014. doi: 10.13189/csit.2014.020403.

[50] Y. Hao, J. Tang, and Y. Cheng. Cooperative sybil attack detection for position based applications in privacy preserved vanets. In *IEEE Global Telecommunications Conference - GLOBECOM*, pages 1–5, Dec 2011. doi: 10.1109/GLOCOM.2011.6134242.

[51] F. A. Ghaleb, A. Zainal, M. A. Rassam, and F. Mohammed. An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In *2017 IEEE Conference on Application, Information and Network Security (AINS)*, pages 13–18, Nov 2017. doi: 10.1109/AINS.2017.8270417.

[52] R. Shrestha, S. Djuraev, and S. Y. Nam. Sybil attack detection in vehicular network based on received signal strength. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 745–746, Nov 2014. doi: 10.1109/ICCVE.2014.7297649.

[53] D. Gantsou. On the use of security analytics for attack detection in vehicular ad hoc networks. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–6, Aug 2015. doi: 10.1109/SSIC.2015.7245674.

[54] A. K. Sharma, S. K. Saroj, S. K. Chauhan, and S. K. Saini. Sybil attack prevention and detection in vehicular ad hoc network. In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pages 594–599, April 2016. doi: 10.1109/CCAA.2016.7813790.

[55] Steven So, Prinkle Sharma, and Jonathan Petit. Integrating plausibility checks and machine learning for misbehavior detection in vanet. *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 564–571, 2018.

[56] Joseph Kamel, Arnaud Kaiser, Ines Ben Jemaa, Pierpaolo Cincilla, and Pascal Urien. CaTch: a confidence range tolerant misbehavior detection approach. In *2019 IEEE Wireless Communications and Networking Conference (WCNC) (IEEE WCNC 2019)*, Marrakech, Morocco, April 2019.

[57] Joseph Kamel. Github repository: Framework for misbehavior detection (f^{2}md), 2019. URL `https://github.com/josephkamel/f2md`.

[58] Joseph KAMEL,Farah HAIDAR, Ines Ben Jemaa, Arnaud Kaiser, Brigitte LONC, Pascal Urien. A Misbehavior Authority System for Sybil Attack Detection in C-ITS. In *IEEE UEMCON 2019*, Octobre 2013.

[59] Framework For Misbehavior Detection (F^{2}MD). F^{2}MD website, 2019. URL `https://www.irt-systemx.fr/f2md`.

[60] C. Sommer, R. German, and F. Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, Jan 2011. ISSN 1536-1233. doi: 10.1109/TMC.2010.133.

[61] L. Codeca, R. Frank, and T. Engel. Luxembourg sumo traffic (lust) scenario: 24 hours of mobility for vehicular networking research. In *IEEE Vehicular Networking Conference (VNC)*, pages 1–8, Dec 2015. doi: 10.1109/VNC.2015.7385539.

[62] VehicularLab. University of luxembourg. URL `http://vehicularlab.uni.lu`.

[63] Jonathan Petit and Raashid Ansari. V2X Validation Tool. `https://bitbucket.org/onboardsecurity/dsrcvt`, BlackHat 2018.

[64] J. Petit, F. Schaub, M. Feiri, and F. Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys Tutorials*, 17(1):228–255, Firstquarter 2015. ISSN 1553-877X. doi: 10.1109/COMST.2014.2345420.

[65] ETSI. ETSI TR 103 415, Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management. 2018.

[66] Yuanyuan Pan, Jianqing Li, Li Feng, Ben Xu. An analytical model for random changing pseudonyms scheme in VANETs. In *2011 International Conference on Network Computing and Information Security (NCIS)*, 2011.

[67] SAMPIGETHAYA K., HUANG ., LI ., POOVENDRAN R, MATSUURA K, SEZAKI K. Providing location privacy for VANET. In *the Third Workshop on Embedded Security in Cars (ESCAR '05)*, 2005.

[68] Karim Emara, Wolfgang Woerndl, Johann Schlichter. CAPS: Context-Aware Privacy Scheme for VANET Safety Applications. In *The 8th ACM Conference on Security Privacy in Wireless and Mobile Networks*, 2015.

[69] A.R. Beresford, F. Stajano. Location Privacy in Pervasive Computing. In *Journal IEEE Pervasive Computing*, 2003.

[70] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos and Jean-Pierre Hubaux. Mix-Zones for Location Privacy in Vehicular Networks. In *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007.

[71] SAE J2735. Dedicated Short Range Communications (DSRC) Message Set Dictionary.

[72] PRESERVE project deliverable D5.3. Deployment issues report v3. 2013.

[73] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, F. Kargl. Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems. In *IEEE Vehicular Networking Conference (VNC'13)*, 2013.

[74] Bjorn Wiedersheim, Zhendong Ma,Frank Kargl,Panos Papadimitratos. Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough. In *The Seventh International Conference on Wireless On-demand Network Systems and Services (WONS2010)*, 2010.

[75] David Forster,Hans Lohr,Anne Gratz,Jonathan Petit, Frank Kargl. An Evaluation of Pseudonym Changes for Vehicular Networks in Large-Scale, Realistic Traffic Scenarios. In *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[76] Karim Emara, Wolfgang Woerndl, Johann Schlichter. Beacon-based Vehicle Tracking in Vehicular Ad-hoc Networks. 2013.

[77] Car 2 Car Communication consortium. https://www.car-2-car.org/.

[78] Deutsches Zentrum für Luft- und Raumfahrt" (German Aeronautics and Space Research Centre - DLR).

[79] C. Sommer, R. German, and F. Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, Jan 2011.

[80] ETSI. TS 102 941, Intelligent Transport Systems (ITS),Security, Trust and Privacy Management. 2018.

[81] ETSI. TS 102 636-6-1 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols. March 2011.

[82] R. Moalla, B. Lonc, H. Labiod, and N. Simoni. Towards a cooperative its vehicle application oriented security framework. In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, 2014.

ECOLE DOCTORALE

Titre: Plateforme de validation des communications sécurisées et de haut niveau de confiance pour les systèmes coopératifs ITS

Mots clés: Cybersécurité, C-ITS, V2X, analyse de risque, attaques

Résumé: Les véhicules de demain seront connectés grâce à plusieurs technologies de communication qui contribue a l'amélioration de la sécurité routière. Le système de transport devient plus ouvert ce qui peut ouvrir la porte à de nouvelles menaces et vulnérabilités qui doivent être prises en compte. La sécurité est un sujet clé à aborder avant le déploiement de STI-C. En plus, la variété des cas d'usage / applications STI-C avec des exigences de sécurité et protection de vie privée différentes, ce qui fait de ces deux derniers des grands défis. Afin de faire face aux problèmes de protection de la vie privée, la solution existante consiste à disposer d'un ensemble d'identités pseudonymes valides, par le véhicule, et de les changer au fur et a mesure de la communication. L'une des motivations de cette thèse est l'analyse des menaces et des vulnérabilités, en particulier celles qui proviennent de l'utilisation des certificats pseudonymes. L'objectif est de mettre en œuvre ces attaques et de proposer des nouvelles solutions, de trouver des améliorations ou des contre-mesures.
La deuxième motivation est d'étudier la performance de la solution existante pour la protection de la vie privée qui est le rechargement des certificats pseudonyms.
La sécurité et la protection de la vie privée dans les STI-C sont considérées comme de grands défis. Beaucoup de travail a été fait et de bonnes solutions existent dans le domaine de la sécurité et de la protection de vie privée. Nous remarquons que les systèmes ne peuvent pas être sécurisés à 100 % mais la sécurité du conducteur est liée à la sécurité du système. Pour cela, le but de cette thèse est de faire du hack blanc du STI-C afin d'améliorer la solution existante. Une évaluation des risques est nécessaire pour identifier notre objectif d'évaluation et analyser les potentiels risques. L'objectif final de cette thèse est de proposer une plateforme de validation qui intégre l'analyse sécurité et l'analyse de performance dans le cadre des STI-C.

Title: Validation platform for secure and highly trusted communications in the context of the Cooperative Intelligent Transport Systems (C-ITS)

Keywords: Cybersecurity, C-ITS, V2X, Risk analysis, attacks

Abstract: Future vehicles will be connected through several communication technologies which will contribute to the improvement of road safety. The transport system becomes more open, this could open the door to new threats and vulnerabilities that must be taken into account. The security protection is a key subject to address before C-ITS deployment. Moreover, the wide variety of C-ITS use cases/application with different security and privacy requirements makes from the security and privacy big challenges.
In order to deal with privacy issues, existing solution consists of having a pool of valid pseudonym identities, by the vehicle, and changing them during the communication. One of the motivations of this thesis is is the investigation on threats and vulnerabilities, especially on those that come from the use of multiple pseudonym identities such as Sybil attack. The objective is to implement those attacks and propose new solutions or find improvements to the existing solution for detecting and preventing security attacks. The second motivation to study the performance of pseudonym certificate reloading. In other words, it is important to ensure that the latency of reloading pseudonym certificates from the PKI while driving at different speeds is acceptable.
A Lot of work has been done and good solutions exist in the security and privacy domain. We notice that systems cannot be secure at 100 % but driver's safety is related to system's security. For this, the aim of this thesis is to do white hack of the C-ITS in order to improve the existing solution. A risk assessment is needed to identify our target of evaluation and analyse potential risks. The final goal of this thesis is to propose a validation plateform that integrates security analysis and performance analysis in the context of C-ITS.