UNIVERSITY CARLOS III OF MADRID

Ph.D. Thesis

Improvements on the enforcement process based on Intelligent Transportation Techniques. Model and mechanisms for electronic reporting, offence notification and evidence generation

Author:

José María de Fuentes García-Romero de Tejada

Supervisors:

Ana Isabel González-Tablas Ferreres, Ph.D.
Arturo Ribagorda Garnacho, Ph.D.

Computer Science and Engineering Department

Leganés, July 2012

TESIS DOCTORAL

Improvements on the enforcement process based on Intelligent Transportation Techniques. Model and mechanisms for electronic reporting, offence notification and evidence generation

Autor:

José María de Fuentes García-Romero de Tejada

Directores:

Prof. Dra. Ana Isabel González-Tablas Ferreres

Prof. Dr. Arturo Ribagorda Garnacho

Firma del tribunal calificador

Presidente:

Vocal:

Vocal:

Vocal:

Secretario:

Calificación:

Leganés, Julio de 2012

A Marité y Manolo, porque sin su sacrificio y dedicación
nunca hubiera llegado hasta aquí.

A Lorena, porque a partir de aquí
espero recorrer el camino a tu lado.

El que no vive para servir, no sirve para vivir.

Agradecimientos

Hace escasamente cinco años terminaba los estudios de Ingeniería Informática. Hoy me encuentro en el escalón siguiente. En esta breve sección (como siempre, una de las que más me cuesta escribir) quiero reconocer a las personas que me han ayudado a llegar hasta aquí. Desde mi punto de vista, esta Tesis es más suya que mía: yo sólo he puesto mi empeño, pero ellos se han preocupado de que pudiera empeñarme en esto.

Lo primero que uno necesita para llegar hasta aquí es *estar vivo*. El primer agradecimiento es para mis padres, **Marité y Manolo**, por darme vida y formarme en todo aquello que los libros no pueden enseñar. Los dos son hoy (sí, en presente: **son**) un referente para mí que me orienta cuando las circunstancias sobrevienen.

Una vez que uno está vivo, necesita estar *preparado*. En este ámbito tengo que reconocer la verdaderamente inestimable labor de mis Directores. Creo que sólo quien ha pasado por esto entiende la relevancia que tiene una tesis, la incertidumbre que lleva asociada y la lucha personal que exige. Por todo ello, tener un Director que empatice contigo, que te oriente (aunque a veces parezca que poco), que jamás ridiculice el trabajo aunque éste sea manifiestamente mejorable (por decirlo suavemente), que te dedique el tiempo necesario como para *hacerte descubrir* el problema y enseñarte cómo se hace una investigación... No tiene precio. **Anabel**: sólo espero tener la oportunidad de recompensar adecuadamente tu esfuerzo y que eso contribuya a asentar definitivamente tu puesto; creo que la Universidad necesita alguien como tú, aunque a veces no se note. Por tu parte, **Arturo**, no sabes hasta qué punto es un privilegio haber sido tu doctorando. No está al alcance de muchos tener un Director que sea una personalidad tan relevante en el área. Gracias por haber depositado tu confianza en mí.

Parte de esa preparación también corresponde a **Benja**, quien en los momentos duros anima, en los fáciles apoya y en los inciertos tranquiliza. En términos técnicos, eres un pleno al quince.

Y por muy vivo y preparado que uno esté, este camino es imposible sin un *acompañamiento.* Gracias a **toda la familia** (hermanos, cuñadas, sobrinas/os) por soportar este intenso periodo de encontrarme siempre en mi cuarto *currando.* Creo que eso no va a variar mucho, tal y como andan las cosas, pero intentaré afrontarlo de una forma más entusiasta.

Dedico un párrafo especial a acompañantes especiales. Un agradecimiento inefable es para **Lorena**. No hay papel para poner ni siquiera la mitad de los motivos. Me quedo con que me has recordado que *La vida es bella*, y solo espero que lo sea para siempre. **Peri, Marcos**, vosotros tenéis un mérito especial por haber estado ahí a pesar de las circunstancias. **Jorge**, tú no te quedas atrás, has sido un compañero de viaje francamente excepcional. Igual que tu tocayo, el **asociado estrella**, que hace que tanto tomarse un mojito como invalidar cualquier firma electrónica sea todo un placer. Prometo ganaros al pádel, si vuestros hombros y rodillas se atreven.

Termino (porque hay que terminar) resaltando al **resto de SeTIanos** (cada uno por un motivo distinto; creo que cada uno sabe el suyo y las necesidades de privacidad me impiden revelarlo), a los miembros de **sub-ARCOS**, a **Mario, Teresa y Pablo**, por los buenos ratos del día a día. Y a la gente de la Universidad de **Siegen** que me brindó un extraordinario acogimiento durante mi estancia.

Abstract

Enforcement activities in the road traffic context have shown to be one of the key factors for reducing fatalities. However, despite their evolution (both in their underlying legislation and their technical means), there are several aspects that may be subject to improvement. Three of them are on the focus of this thesis. First, victims of offenders are usually not able to report them, as there are not enough data to support their claims. Second, there is a significant delay between the offence and its notification, which negatively affects to its educational purpose. Third, the offender does not have the practical chance to defend herself (i.e. claim her innocence or, at least, that it was a less serious offence) as there are no suitable attesting elements.

In order to contribute on these issues, recent advances on data processing, communication and sensing capabilities of vehicles conform an interesting technological context. These new capabilities are the basis over which a new family of services, called Intelligent Transportation Systems (ITS) are being developed. Despite the new opportunities provided by ITSs, it does not exist an adequate framework to guide the introduction of these new techniques in the surveillance of the adherence to the road traffic rules. Thus, there is a lack of a clear view on how these techniques may help on the aforementioned problems.

The general goal of this thesis is to provide the technical basis for the realization of an ITS-enhanced electronic road traffic administrative enforcement process. Particularly, four contributions are developed in this thesis. First, an enforcement process model is proposed, based on the results of the European VERA2 project. The model describes the entities, the stakeholders, the data at stake and the underlying security considerations. It conforms the aforementioned framework that enables identifying where to introduce the required ITS enhancements.

Based on the previous model, the remaining contributions focus on the development of specific mechanisms where the enforcement actors (the offender, the offence witnesses, the victims and the Authority) participate actively through ITS-related technologies. Thus, the second contribution is a mechanism that enables victims to report their offenders. In order to prevent this action to be noticeable by the reported driver, the report information is embedded into innocuous-looking messages by means of steganography. As the educational purpose of the punishment grows with its immediacy, the third contribution is a protocol to send an offence notification to the offending vehicle. Thanks to the human-machine interface of the vehicle, the offender is able to realize about the fine even during the same trip in which the offence was committed. Finally, in order to ensure that the driver has adequate means to defend herself against unfair punishments, a protocol to create evidences on its recent driving behavior has been proposed. Such evidences are based on the sensorial perceptions by surrounding vehicles, which are contacted using ITS communication technologies.

At the light of these contributions, this thesis opens the door to upcoming developments that may end into a fully automated enforcement process.

Keywords: Enforcement process, Intelligent Transportation Systems (ITS), Vehicular Ad-hoc Networks (VANET)

Resumen

Uno de los factores más criticos para la reducción de la siniestralidad en las carreteras es la vigilancia del cumplimiento de las normas de circulación. A pesar de la evolución de los procedimientos y técnicas para efectuar dicha vigilancia (tanto en el ámbito normativo como en el técnico), existen algunos factores que son susceptibles de mejora. Tres de ellos constituyen el foco principal de esta tesis. En primer lugar, las víctimas de los infractores no disponen de medios prácticos para denunciarles, pues habitualmente no existen datos que permitan acreditar la descripción de los hechos manifestada. En segundo lugar, existe un intervalo significativo de tiempo entre la comisión de la infracción y la recepción de la notificación de la correspondiente denuncia, lo que afecta negativamente a la capacidad educativa de las sanciones. En tercer lugar, el supuesto infractor no dispone de medios prácticos para defenderse, pues habitualmente no se cuenta con elementos que soporten su argumento.

Con el fin de contribuir a estas cuestiones, los avances recientes en materia de procesamiento de información, transmisión de información y percepción sensorial en los vehículos constituyen un contexto tecnológico interesante. Estas nuevas capacidades son la base sobre la que se construyen los Sistemas Inteligentes de Transporte (habitualmente referidos mediante sus siglas en inglés, ITS). A pesar del desarrollo constante de dichos sistemas, no existe un marco adecuado para la utilización de dichas capacidades en el ámbito de la vigilancia del cumplimiento de las normas de circulación. Así, se detecta una carencia de una visión clara de cómo estas nuevas técnicas pueden contribuir a resolver los aspectos problemáticos identificados anteriormente.

El objetivo general de esta tesis es proporcionar la base técnica para el desarrollo de un procedimiento administrativo sancionador en el ámbito del tráfico que aproveche las oportunidades que plantean los ITS. En particular, en esta tesis se desarrollan cuatro contribuciones. En primer lugar, se propone un modelo de procedimiento administrativo sancionador, extendiendo los resultados del proyecto de investigación europeo VERA2. Este modelo describe las entidades participantes, los interesados, la información en juego y las consideraciones de seguridad subyacentes. Este modelo constituye el antedicho marco y permite identificar la forma de introducir las tecnologías ITS en dicho proceso.

Basándose en este modelo, las contribuciones restantes se centran en el desarrollo de mecanismos específicos en los que los actores del proceso (el infractor, los testigos, las víctimas y la Autoridad) participan activamente empleando tecnologías relacionadas con los ITS. Así, la segunda contribución es un mecanismo que permite a las víctimas denunciar a los infractores. Con el objetivo de impedir que dicha denuncia sea conocida por el infractor, el mensaje es introducido mediante técnicas esteganográficas en otro mensaje aparentemente inofensivo. La tercera contribución es el envío de la notificación de forma directa al vehículo infractor, lo cual pretende incrementar la inmediatez del proceso (ya que se le puede presentar al infractor durante la conducción) y, con ello, su eficacia educativa. Finalmente, para promover que el conductor disponga de los medios adecuados para defenderse de sanciones supuestamente injustas, se propone un protocolo para la creación de evidencias que describan su comportamiento reciente en lo que respecta a la conducción. Dichas evidencias se basan en las percepciones sensoriales de los vehículos cercanos, los cuales son contactados empleando tecnologías de comunicación relacionadas con los ITS.

A la vista de estas contribuciones, esta tesis abre la puerta al futuro desarrollo de un proceso sancionador completamente automatizado.

Palabras clave: Procedimiento sancionador, Sistemas Inteligentes de Transporte (ITS), redes vehiculares (VANET).

Contents

List of Figures

List of Tables

Part I

Introduction

Chapter 1

Introduction

This Chapter introduces the context of the thesis, the statement of the problem, the main objectives of the thesis, the contributions achieved and the document organization.

1.1 Context

Nowadays, Information and Communication Technologies (ICT) are being more and more integrated in daily activities of modern societies. One of such activities is the public government, which is evolving towards the concept of e-government, defined by the OECD (Organisation for Economic Co-operation and Development) as the *use of ICT, specially Internet, as a tool to achieve better government* [1].

The thesis is related to a particular process within the e-government: the enforcement process. Specifically, the focus is on the road traffic administrative enforcement one. There are two main issues in the context of this thesis, namely the legal provisions and the technical environment (see upper part of Figure 1.1). Concerning the legal issues, the regulations of the enforcement process define how it must work in order to be valid. With respect to the technical issues, the approach selected in this thesis is based on *Intelligent Transportation Systems* (ITS). According to the definition provided by the European Parliament, ITSs *are advanced applications that without embodying intelligence as such aim to provide innovative services on transport modes and traffic management and enable various users to be better informed and make safer, more coordinated and "smarter" use of transport* *networks* [2].

Both the legal and technical issues are the main inputs required to design any enhancement in the enforcement process. It should be noted that both areas are not independent, but instead they are related to another area – the ICT security issues. They comprise the *study of the protection methods and mechanisms against revealing, alteration or destruction of the data at stake.* It also covers the *failures in the processing, storage or transmission of such data* [3]. Thus, the legal nature of the enforcement process and its underlying data at stake imposes a set of security requirements to be addressed in the technical environment. OECD states that security and privacy issues have to be addressed prior to the development of any electronic process within the e-administration [1].

In order to give an overview of such related legal and technical issues, the following Sections present a brief introduction of each one.

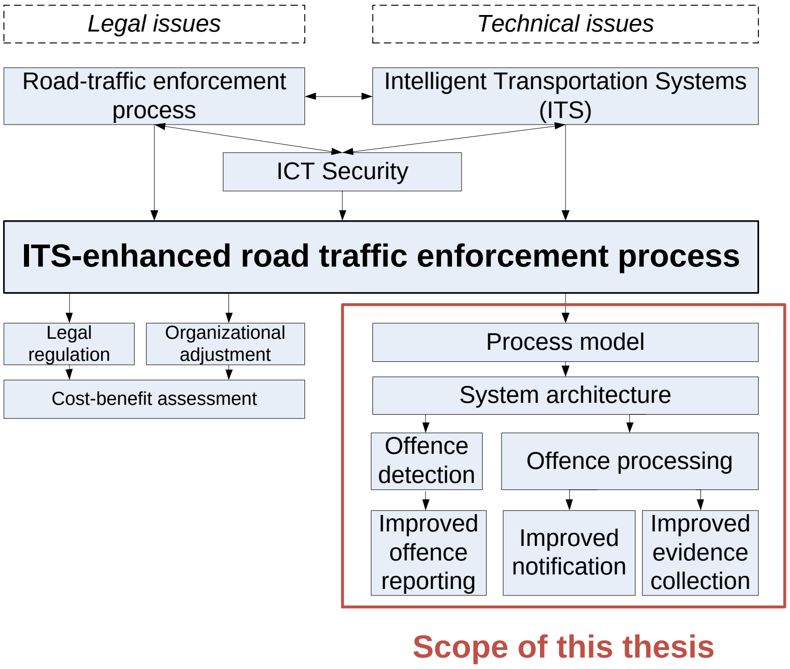

Legal issues
Technical issues
Road-traffic enforcement process
Intelligent Transportation Systems (ITS)
ICT Security
ITS-enhanced road traffic enforcement process
Legal regulation
Organizational adjustment
Cost-benefit assessment
Process model
System architecture
Offence detection
Offence processing
Improved offence reporting
Improved notification
Improved evidence collection
Scope of this thesis

Figure 1.1: Context and scope of this thesis

1.1.1 Legal issues

The road traffic administrative enforcement process is applied to all traffic offences detected by the Authority that are not considered as criminal. For example, light speeding is considered as an administrative offence in several European countries.

Enforcement activities have been shown to be one of the key factors in reducing traffic fatalities [4]. The effectiveness and efficiency of such procedure are critical to ensure the educational capacity of sanctions. To achieve these goals, the Spanish Law 11/2007 enabled the use of electronic means in the administration (and thus, in all its processes), not only for internal application but also for the communication with citizens [5]. Apart from the use of electronic means, the road traffic enforcement process was recently reformed in 2009, aiming to simplify the process while preserving the underlying legal provisions [6]. This reform is also intended to help offenders to know whenever they are involved in such a process.

The active participation of the citizen within the process has been taken into account in its design. Thus, all phases enable stakeholders to participate. On the one hand, offenders may defend their interests, giving more data or appealing existing arguments in order to guarantee that the imposed fine is accurately established according to the severity of the facts. On the other hand, citizens have the chance to report offences witnessed by them.

1.1.2 Technical issues

In order to develop the aforementioned ITS applications and services, it is necessary to explode the growing data processing and communication capabilities of vehicles. Concerning data processing, vehicles are incorporating a growing number of electronic devices, in form of sensors, embedded systems and processors. They are included to increase the comfort and safety, as well as assisting the driver in her task. Moreover, a growing number of vehicles already incorporate electronic devices that record the vehicle driving behavior (e.g. speed, last actions, use of brakes or warning lights, etc.) [7].

With respect to the communication features of vehicles, they incorporate one device usually referred to as On-Board Unit (OBU). Such device enables them to exchange data not only with other (nearby) vehicles, but also with a dedicated infrastructure arranged along the roads. Through this infrastructure, vehicles can interact with ITS service providers. This kind of communication has given place to the vehicular network, which is a specific type of network that is adapted to the special features of this environment (i.e. mobility, amount of nodes, etc.).

All these technologies are being developed taking into account the underlying data security issues. Great investments are being performed by carmakers, as well as research institutions, to achieve a high level of security. In fact, the IEEE 1609 family of standards on vehicular networks contains one (IEEE 1609.2) specifically focused on data security [8].

1.2 Motivation

The general purpose of this thesis is related to the improvement of the road traffic administrative enforcement process. Particularly, there are two areas of the current road traffic administrative enforcement process that may be subject to improvement – its *immediacy* and the *citizen interaction* on it. Concerning the first one, the European Commission has pointed out the need for offences “to be notified and sanctions to be executed within a short time period” [9]. To this regard, European research projects such as ESCAPE (Enhanced Safety Coming from Appropriate Police Enforcement) have highlighted the benefits of automatising this process [4]. The use of electronic means within the process, as mandated by Law 11/2007, allow for a moderate reduction of processing times. However, this reduction is currently insufficient for the specific area of road traffic. It must be noted that this specific field requires greater immediacy as the reappearance of the punishable behaviour may lead to serious damage to other road users.

Regarding the citizen interaction, it is currently not possible to have a real-time interaction between all the stakeholders involved in a traffic offence, namely the offender, witnesses, the affected victim(s) and the road traffic Authority. In fact, current communication with the Authority usually implies a non-negligible time period, which makes the process to last for a long time.

The previous issues, along with the fact that ITS technologies may be applied to solve them, have led us to detect four specific problems that need to be addressed.

P1. Lack of a complete enforcement process model that helps on identifying the chances to integrate ITS technologies in this context

In order to improve the enforcement process, the VERA series of projects (Video Enforcement for Road Authorities) focused on the cross-border enforcement, that is, to ensure that an offence committed by a foreign driver is punished in its country of residence. Particularly, the VERA2 project proposed an enforcement process model consisting of a set of flowcharts and a data dictionary [10]. Such flowcharts constitute a basic model, as it details *what* has to be done. However, it does not specify *how* to perform each step nor its involved data. On the other hand, concerning the data dictionary, it covers the data elements that may be sent between countries for delegating the enforcement. Thus, it does not contain all elements produced in each process phase that is addressed in a single country. In this situation, the VERA2 model is not enough to clarify how to integrate ITS techniques in this process and, in fact, this issue is not addressed by such project.

P2. Victims of offenders do not have the practical chance to report such misbehavior

From the legal point of view, any person that knows about a traffic offence is enabled to report it to the Authority [6]. However, in practice, there is no practical mechanism to perform this operation. The situation is particularly worse in the case of drivers that suffer the consequences of the traffic offence. As their task is focused on driving, they may proceed with the reporting once the car is stopped. In this way, they are forced to memorize all the data related to the offence (e.g. involved cars, date, location, event description), which in practice is not usually performed. Furthermore, there is a need to attest the claimed description in order to prevent unsupported reports. According to data provided by the Spanish National Traffic Authority for the context of this work, most voluntary reports are discarded because of the lack of supporting evidences[1].

P3. Current notification mechanisms cause offenders to be aware of the punishment long after the offence

Existing legislation enables the use of not only regular (i.e. paper-based postal services) mechanisms, but also electronic ones, to deliver a fine notification. All these alternatives introduce a time gap. On the one hand, the postal service may take up to some days. On the other, even if the electronic notification may be performed in the order of minutes, the current goal of the Spanish Traffic Authority is to reduce this gap from 45 days to 12 [11]. This does not seem a very convenient goal from the road safety point of view, because the immediacy of the notification has a positive effect on its educational effect [4]. Thus, previous theoretical works have pointed out that the immediacy of feedback after an offence is crucial to promote a higher behavioural impact[2] [13]. The most convenient goal should be to make this effect to be real as soon as possible, even within the same trip in which the offence was committed. Such time reduction could also help drivers to defend themselves, as the moment of the offence would be more recent [14].

Apart from the previous fact, current mechanisms enable a *passive behavior* from the offender side. In this way, she is allowed to not taking any decision regarding the notification (i.e. neither accepting nor rejecting it). In this particular case, the offender is *never* aware of such notification and she will only be once the process reaches the next notifiable state.

P4. Drivers do not have effective mechanisms to defend themselves

[1] This information was provided to the author of this thesis in a private e-mail conversation with the Chief of Research and Studies of the Spanish Road Traffic Safety Observatory.

[2] For a detailed explanation of the underlying behavioural mechanisms, please refer to [12].

against received fines

Once a traffic fine is received, drivers have the right to give evidences and allegations that may offer another view of the facts. Their main purpose is to clarify the situation, potentially leading to a fine reduction or removal. Nevertheless, there is currently no practical mechanism to create these defensive elements that help the driver on attesting its driving behavior or the surrounding circumstances. What is more, the legislation determines that the truth of the facts given by type approved equipments or police officers leaves *little room for doubt* [6].

To illustrate this fact, in 2006 the Spanish Traffic Authority imposed 2.588.890 fines, and only 148.066 (i.e. 5,71 % of the total) were contested [15]. Nevertheless, 36.4 % of drivers believe that it is an unfair enforcement system, according to a survey conducted by the Traffic Authority [16]. It would be expected that such a significant proportion of unsatisfied drivers be followed by a proportional amount of contests, if it were practical to proceed.

1.3 Objectives and contributions

The general goal of this thesis is to provide the technical basis for the realization of an ITS-enhanced electronic road traffic administrative enforcement process. Particularly, the intended consequence is to enable an enriched real-time interaction with the stakeholders related to a given traffic offence. In this way, offences are rapidly reported (even by witnesses) and notified to the offender, who is now enabled to defend herself.

In our opinion there was a need to address the previous research topics, which have been reflected in the objectives of this thesis:

O1. Design a **complete model of the enforcement process** that helps to identify the **chances to integrate ITS-related technologies**.

O2. Create a **mechanism** that enables **victims of misbehaving drivers to report them**. It should ensure that this action is not likely to be noticeable by the reporting driver.

O3. Create a **mechanism** to deliver the **notification to the vehicle** respecting the legal requirements. It should promote the immediacy of the process.

O4. Create a **mechanism** that enables **drivers to build electronic evidences** attesting their driving behaviour. The reliability of the created evidences must be characterized. The verification process should be defined as well.

The achievement of these objectives has led to the next four contributions:

C1. An **enhanced enforcement process model based on the VERA2 one** (see Chapter 4) that describes the phases, the data at stake, the data exchanges and the underlying security considerations. This model will be focused on speeding offences, based on the corresponding model proposed in the aforementioned VERA2 project. Nevertheless, it is expected that other traffic offences will follow a similar process, although such issue is a matter of future work. The suitability of the proposed model to represent current enforcement systems (particularly the Spanish ESTRADA and the French CSA) is evaluated. In general words, almost all functionalities have been identified in the proposed model. Only two components were not successfully identified – one because of the lack of detail on the aforementioned systems and the other because it was out of the scope of the CSA one. As a result, the suitability of these parts of the proposed model is not completely contrasted. Furthermore, based on this model, the integration of ITS-related technologies is analysed, as well as their suitability compared to current approaches. In general words, although ITS requires a non-negligible investment, it enables a greater immediacy in the offender identification and in the notification process. Furthermore, it promotes having a more complete description of the offence.

C2. An **application of steganographic principles** to ITS-related messages (see Chapter 5) that enables vehicles to embed data within them. For the context of this thesis, this mechanism enables **reporting other misbehaving vehicles** by embedding their current identifier and the type of misbehavior perceived. The approach is to embed such information into beacon messages. The scope of this mechanism is the embedding and revealing operations. Therefore, the posterior processing of the embedded report and particularly its trustworthiness analysis is left to future work. Results show that the proposed steganographic system is computationally feasible taking into account realistic vehicular constraints (processing capabilities, communication reliability and bandwidth), and that at least one configuration setting exists in which the system is operational for common scenarios (highways, secondary roads and urban environments). The analysis of the imposed requirements shows that the undetectability is subject to ensuring that sensor errors are truly random and that the future improvement of sensor accuracy will reduce the capacity of this mechanism.

C3. A **protocol to send an offence notification to the offending vehicle** by means of ITS-related communication media, respecting the security requirements derived from the legal provisions for the validity of the notification (see Chapter 6). The impact of the protocol on vehicular devices and communication channels is evaluated. The analysis shows that the proposed protocol fulfils all security requirements that do not require a real implementation for their validation. Regarding its performance, results show that in absence of OBU compromise, the notification message must be sent 7 times to achieve a probability of successful transmission of 99%. Concerning the processing costs, it takes around 1.46 seconds for the vehicular computational device.

C4. An **inter-vehicle protocol** (called EVIGEN, see Chapter 7) that **enables a vehicle to build an evidence** of its recent driving behavior by retrieving the sensorial **perceptions of surrounding vehicles**. The protocol covers not only the evidence creation but also its verification. Nevertheless, the trustworthiness evaluation of the data provided by such surrounding vehicles is left to future work. The suitability of the protocol for vehicular networks and computational devices is analysed. The amount of available witnesses depends on the gap between the moment to which the evidence may be referred and the time in which the evidence is requested to witnesses. Simulation results show that for an interval of 5 seconds, 90 % of witnesses are available in urban environments and a maximum average of 38 testimonies per evidence is achieved in highways. Other road scenarios and time gap options are also analysed. The security analysis shows that all requirements are adequately fulfilled and thus the associated threats are countered.

The relationship between the problems detected, the research objectives and the contributions achieved is shown in Table 1.1.

Problem	**Objective**	**Contribution**
P1. Lack of a complete model of the enforcement process	O1. Design a complete model	C1. Enhanced enforcement process model based on the VERA2 one
P2. Lack of a practical technique to report misbehaving drivers by their victims	O2. Creation of a mechanism for inter-vehicle reporting	C1. Enhanced enforcement process model based on the VERA2 one C2. Steganography-based protocol for covert inter-vehicle reporting
P3. Time gap between offence and fine notification	O3. Improve the immediacy of notification mechanisms	C1. Enhanced enforcement process model based on the VERA2 one C3. Protocol to send an offence notification to the offending vehicle
P4. Lack of self-defending mechanisms for drivers	O4. Design of a mechanism that enables drivers to create evidences	C1. Enhanced enforcement process model based on the VERA2 one C4. EVIGEN protocol for co-operative evidence generation

Table 1.1: Relationship between problems, objectives and contributions

We find that these issues are a step towards the complete automation of the road traffic enforcement process. Figure 1.2 shows the improvements that are enabled in such a process by means of the mechanisms proposed in this thesis. Therefore, the process may now be started by every vehicle that detects an offence (step 1 in Figure 1.2, contribution 2). Once the verifier has checked the authenticity of the report, the adjudicator prepares and sends the offence notification (step 2, contribution 3). Finally, the offender may create an electronic evidence in order to defend herself, in the case that she finds that the offence is unfair (step 3, contribution 4).

The scope of the proposed mechanisms is on the data processing and exchange, leaving out its trustworthiness analysis. Thus, the reporting mechanism and, particularly, the operations described to retrieve such report, does not address how the verifier decides about the reliability of the report. Analogously, once a notification is received, the decision algorithm to establish whether it is fair or not is not considered. Similarly, the reliability analysis of the data provided by vehicles for building the electronic evidence is not detailed. It should be noted that this kind of evaluation is a matter of open research. Currently, plausibility checks (e.g. [17]) and reputation-based mechanisms (e.g. [18]) are two significant trends on this area.

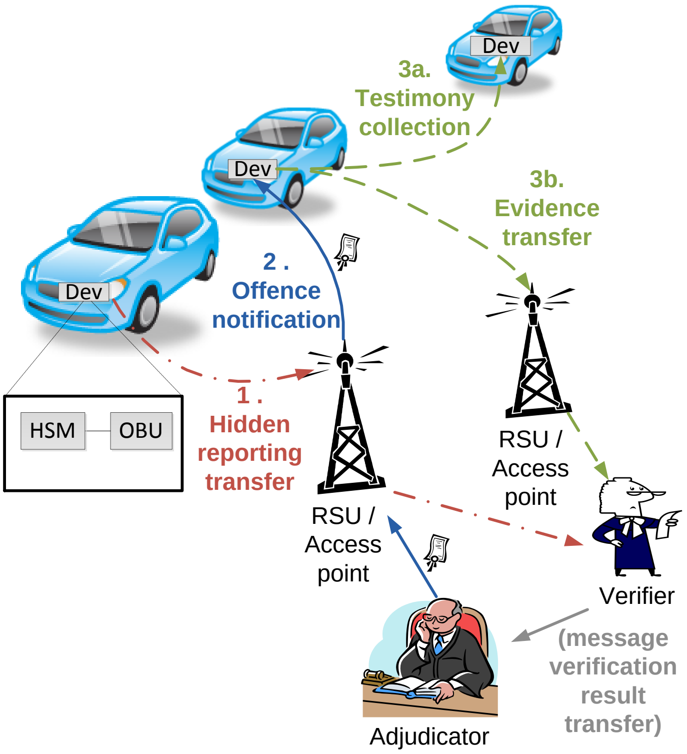


Figure 1.2: Graphical view of the contributions 2, 3 and 4 of this thesis

It must be noted that the automation of the road traffic enforcement process is one of the goals of the research project “Security Architecture and generation of forensic electronic evidences in vehicular environments” (E-SAVE), which is funded by the Spanish Ministerio de Ciencia e Innovacion under grant TIN2009-13461. Therefore, this thesis is conducted within the scope of such research project.

The research results published in scientific journals and conferences during the development of the present thesis are listed in Appendix B.

1.4 Document organization

This thesis is composed by several chapters distributed along five parts:

Part I. Introduction. This part introduces the whole document, and contains the present Chapter.

Chapter 1. Introduction. This is the present Chapter, and contains the thesis context, the statement of the problem, the research objectives and the main contributions achieved.

Part II. State of the art. This part analyses the state of the art that is closely related to this thesis. The reviewed topics have been organised into two chapters.

Chapter 2. Intelligent Transportation Systems and Vehicular networks. This chapter describes the technological context of this thesis concerning the vehicular technology. It introduces the main concepts and technologies that are used in the contributions presented in this work. The related security issues are also presented herein.

Chapter 3. Enforcement process. Technical and legal issues. This chapter introduces the enforcement process, its particular realization in Spain and the legal provisions regarding the electronic notification and the electronic evidence.

Part III. Proposal. This part includes the proposal elaborated to fulfil the research objectives established above. Each of the four contributions is presented in a separate chapter.

Chapter 4. Enhanced road traffic administrative enforcement process model for speeding offences and ITS realization. In this Chapter, an enhanced enforcement model is proposed based on the previous VERA2 one. The stakeholders, the enforcement entities, the data at stake including their interchanges and their security and privacy concerns are also addressed. Based on this model, it is discussed how ITS technologies may help on addressing the problems of this process. Furthermore, this Chapter describes the parts of the model that are related to each of the remaining contributions. Moreover, the decisions and assumptions taken over the vehicular scenario for the remaining contributions of this thesis are also introduced here.

Chapter 5. Mechanism for covert reporting of misbehaving vehicles. This Chapter describes the steganography-based mechanism proposed to enable victims of offenders to covertly report them. The details on the cover message selected, its capacity, the selected protection mechanism and the embedding and revealing functions are presented herein.

Chapter 6. Vehicular-enhanced electronic notification protocol. The proposed electronic notification protocol is described here. For this purpose, the considered model is presented, along with the architecture and a comparison with other alternatives. The protocol itself is formalized at the end of this Chapter.

Chapter 7. EVIGEN: A protocol for vehicular cooperative EVIdence GENeration. The protocol proposed to enable the generation of evidences describing a recent driving behavior by a vehicle (in this context, specially the offender) is described in this Chapter. The model, architecture and protocol steps are presented herein, along with a discussion on different design alternatives.

Part IV. Evaluation and Conclusions. The evaluation of the thesis contributions and the conclusions are presented in this part, which is formed by two chapters.

Chapter 8. Evaluation. This Chapter contains the evaluation of the thesis contributions:

– The enforcement model. It is assessed its suitability to represent current enforcement systems, and the suitability of ITS techniques in this context.

– The reporting mechanism. It is analyzed its computational and operational feasibility, its robustness and the fulfilment of the identified security requirements.

– The notification protocol. The achievement of the security requirements derived from the legal provisions is verified. Furthermore, the computational and network impact for different degrees of probability of success is measured, considering the unreliability of the vehicular communication network.

– The evidence generation protocol. It is evaluated its suitability to different road scenarios. The amount of testimonies and witnesses available under different assumptions is evaluated. The security requirements are also analysed.

Chapter 9. Conclusions and Future Work. In this Chapter, the conclusions of this thesis are provided. A critical discussion of the work performed in this thesis is presented. In addition, future research directions that may be derived from this thesis are outlined.

Part V. Bibliography and Appendices. This part includes the bibliography in use, the scientific publications derived from the underlying research, and a set of appendices that complement the main content.

Bibliography. The bibliography contains the list of references to other research papers, technical documents and standards used in the thesis.

Acronyms and abbreviations The set of acronyms and abbreviations that are used throughout this thesis are presented herein.

Publications. The papers related to this thesis work in which the author has participated are listed herein.

Specification of the data exchanges in the proposed model. This Appendix complements the proposed model in Chapter 4.

Part II

State of the art

Chapter 2

Intelligent Transportation Systems and Vehicular networks

The increasing demand for connectivity due to the evolution of the Information Society leads to the emergence of new communication scenarios. These are increasingly integrated in the environment, giving access to networks anytime and anywhere. Because of this constant change, some daily activities are evolving to incorporate data sharing in its development. In the last years, this trend is being also present in the vehicle and its environment. It is expected that both the traffic management and the driving task are simplified with this technical improvement.

This Chapter introduces, first, the main concepts related to these new services, called Intelligent Transportation Systems (Section 2.1). Some representative applications related to enforcement are also described therein. As these services are usually based on a specific type of communication network referred to as Vehicular Ad-hoc Network (VANET), it is briefly described in Section 2.2. Given the incidence of security issues of such network in the contributions of this thesis, they are introduced in Section 2.3.

2.1 Intelligent Transportation Systems

2.1.1 Description

The European Parliament, in its Directive on Intelligent Transportation Systems (ITS) of 2009, defined these systems as *advanced applications that without embodying* *intelligence as such aim to provide innovative services on transport modes and traffic management and enable various users to be better informed and make safer, more coordinated and "smarter" use of transport networks* [2].

Such applications enable improvements over traditional procedures, such as accident reconstruction. For example, previous works have focused on combining the vehicle-provided data with other information received from other vehicles in order to rebuild the situation [19].

For these applications to be real, there is a set of enabling technologies that are in constant evolution. Thus, vehicles are equipped with a growing set of sensors that enable them to perceive their status and its surroundings [7]. Moreover, they are equipped with a computational device and a communication unit that allows them to exchange information with other nodes.

2.1.2 ITS applied to promote compliance to traffic rules

There are several applications devoted to promote the driver's compliance to traffic rules. Thus, *Intelligent Speed Adaptation* (ISA) tries to ensure that the vehicle is being driven at a safe speed. For this purpose, the vehicle either receives the speed limit in force from a service provider, or it has this information pre-loaded (for example, in the navigation system). ISA systems may also be classified according to the level of intervention in the driving task. Thus, they may be limited to informing the driver whenever she is speeding (passive ISA) or they may actively decrease the speed once it happens (active ISA).

On the other hand, *in-vehicle signage* is intended to electronically transmit the speed limit to passing by vehicles. In this way, the driver may be informed using the human-machine interface of the vehicular communication systems. Thanks to this application, the driver does not have to memorize the speed limit in force and, moreover, dynamic speed limits may be implemented without requiring the driver to pay excessive attention to the current limit.

Finally, the Electronic Fee Collection (EFC) is a widespread tolling system that enables an electronic payment of the entrance fee that is applied in some highways. Thus, the vehicle electronically interacts with the toll booth and performs the vehicle's authorization of payment, which also requires its identification.

At the light of these descriptions, it is possible to identify that ITS systems are intended to *assist* the driver (passive ISA, in-vehicle signage), to *correct* the driver actions (active ISA) or even to *act on behalf* of the driver (EFC).

2.2 Overview of vehicular networks

VANETs are considered as a specific type of mobile network (in English, Mobile Ad-hoc NETwork) [20]. In the following subsections, the entities that participate in such network are introduced (Section 2.2.1), as well as their communication patterns (Section 2.2.2). The specific challenges that are faced by these networks are described in Section 2.2.3. Finally, Section 2.2.4 is devoted to the devices that a vehicle uses to actively participate in a VANET to receive any ITS service.

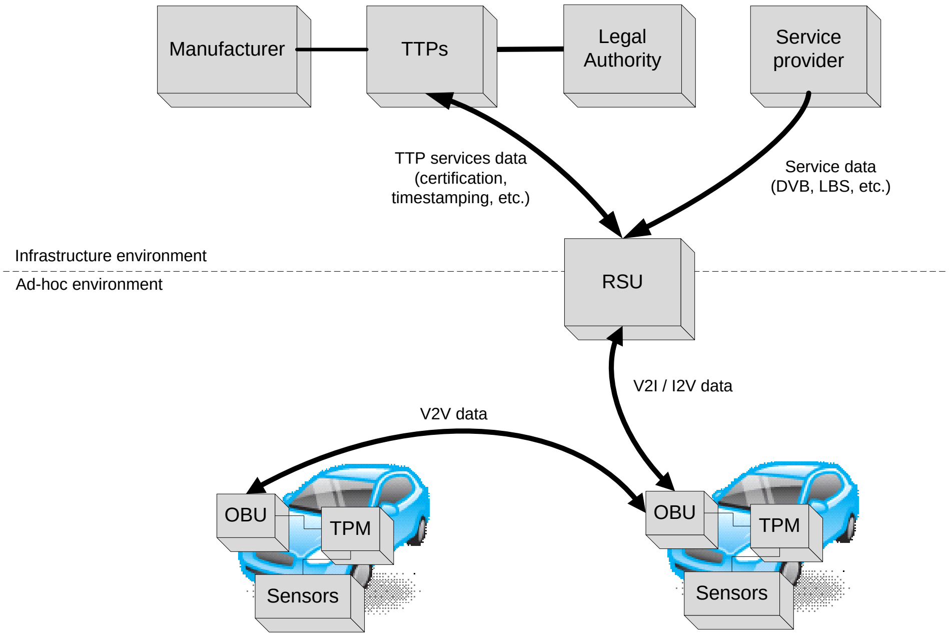


Figure 2.1: Overview of a vehicular network

2.2.1 VANET entities

Several different entities are usually assumed to exist in VANETs. To understand the internals and related security issues of these networks, it is necessary to analyze such entities and their relationships. Figure 2.1 shows the typical VANET scheme, where two different environments are generally considered:

Infrastructure environment. In this part of the network, entities can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. On one hand, manufacturers are sometimes considered within the VANET model. As part of the manufacturing process, they identify uniquely each vehicle. On the other hand, the legal authority is commonly present in VANET models. Despite the different regulations on each country, it is habitually related to two main tasks - vehicle registration and offence reporting. Every vehicle in an administrative region should get registered once manufactured. As a result of this process, the authority issues a license plate. On the other hand, it also processes traffic reports and fines. Trusted Third Parties (TTP) are also present in this environment. They offer different services like credential management or timestamping. Both manufacturers and the authority are related to TTPs because they eventually need their services (for example, for issuing electronic credentials). Service providers are also considered in VANETs. They offer services that can be accessed through the VANET. Location-Based Services (LBS) or Digital Video Broadcasting (DVB) are two examples of such services.

Ad-hoc environment. In this part of the network, sporadic (ad-hoc) communications are established from vehicles. Apart from other devices (that will be introduced in Section 2.2.4), vehicles are equipped with a communication unit (OBU, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. Such infrastructure is formed by some communications devices located aside the roads, called Road-Side Units (RSU). In this way, RSUs become gateways between the infrastructure and vehicles and vice versa.

2.2.2 VANET communication patterns

Depending on the nature and purpose of each ITS application, the way in which messages have to be spread may be different. Four different communication patterns may be identified in these networks.

- V2V warning propagation. There are situations in which it is necessary to send a message to a specific vehicle or a group of them. For example, when an accident is detected, a warning message should be sent to arriving vehicles to increase traffic safety. On the other hand, if an emergency public vehicle is coming, a message should be sent for preceding vehicles. In this way, it would be easier for the emergency vehicle to have a free way. In both cases, a routing protocol is then needed to forward that message to the destination.

- V2V group communication. Under this pattern, only vehicles having some features can participate in the communication. These features can be static (e.g. vehicles of the same enterprise) or dynamic (e.g. vehicles on the same area in a time interval).

- V2V beaconing. Beacon messages are sent periodically to nearby vehicles. They contain the current speed, heading, braking use, etc. of the sender vehicle. These messages are useful to increase neighbor awareness. Beacons are only sent to 1-hop communicating vehicles, i.e. they are not forwarded. In fact, they are helpful for routing protocols, as they allow vehicles to discover the best neighbor to route a message.

- I2V/V2I warning. These messages are sent either by the infrastructure (through RSUs) or by a vehicle when a potential danger is detected. They are useful for enhancing road safety. As an example, a warning could be sent by the infrastructure to vehicles approaching to an intersection when a potential collision could happen.

2.2.3 Challenges of this type of network

VANETs have to face three main challenges that are not common in other network environments – the *mobility of some nodes*, the *network volatility* and the *concentration of nodes*. Concerning the mobility, it must be noted that vehicles move at high speed (and can even exceed 120 kmph) and with different itineraries. The network volatility is caused because in such networks the existence of a stable communication infrastructure is not assumed. The aforementioned high mobility of vehicles, with their limited communication range, causes the networks to be established in an *ad-hoc* fashion, that is, networks of a limited temporal scope. Finally, many vehicles can concentrate in one area (e.g. at traffic lights or in a traffic jam), leading to networks with a large number of nodes.

2.2.4 In-vehicle devices required to participate in a VANET

Apart from the aforementioned OBUs, there are other in-vehicle devices that are related to the participation in ITS applications and their underlying communication networks. Such devices are organized following an in-vehicle architecture. The OVERSEE project[1] proposes an architecture that focuses on security issues. Particularly, OVERSEE proposes a three-layer architecture, where the software and hardware components are connected through a middleware layer (Figure 2.2). The middleware ensures data confidentiality and integrity, as well as reliable message delivery between sender and receiver.

In the software layer, there are three main components, namely the cryptographic module, the secure I/O partition and the secure application partition environment. The cryptographic software is the only component that may access to the Hardware Security Module (HSM), in order to perform the cryptographic needs that are defined in IEEE 1609.2. HSMs are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable

[1] https://www.oversee-project.com/

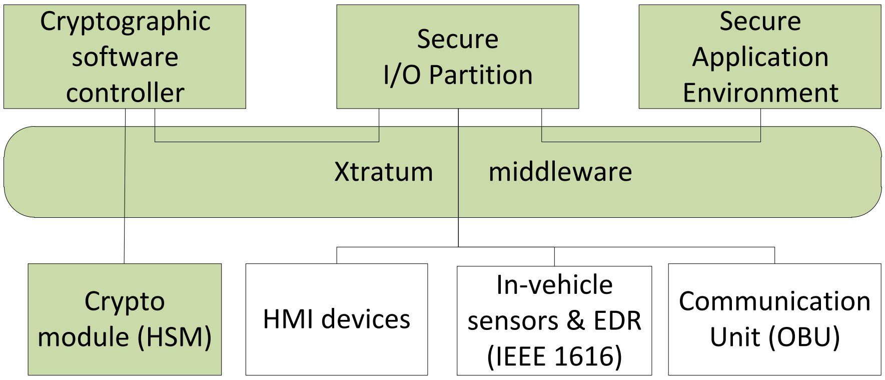

Cryptographic software controller
Secure I/O Partition
Secure Application Environment
Xtratum middleware
Crypto module (HSM)
HMI devices
In-vehicle sensors & EDR (IEEE 1616)
Communication Unit (OBU)

Figure 2.2: Elements of the OVERSEE in-vehicle architecture related to this thesis

internal clock and are supposed to be tamper-resistant or at least tamper-evident [21]. In this way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored. The secure I/O partition establishes the access control mechanisms to ensure that only the authorized applications make use of the different in-vehicle devices such as in-vehicle sensors (which are connected to a recorder component called Event Data Recorder [22]) or human-machine interface devices. The Secure Application Environment (SAE) contain the software that implements the different services offered to the driver. Other non-secured environments (called *partitions*) are devised by OVERSEE for applications that do not require security. Given that the mechanisms proposed in this thesis are related to the enforcement process, their security needs impose that the corresponding application code be in this secured environment.

In order to clarify the terminology, some projects use the term OBU to refer to the whole set of the aforementioned in-vehicle devices. For example, the tolling device developed by Toll Collect in Germany[2] is referred to as OBU, and it is in charge of not only the transmission but also the processing of the data at stake. In this thesis, according to the definition provided by standard IEEE 1609.1, the OBU only refers to the communication unit [23].

The inherent security properties offered by the HSM are the ultimate security

[2] http://www.toll-collect.de/en/home.html

guarantee of the complete system. Thus, the system is booted in the following way. Before starting the system, it is assumed that the root public key certificate of the HSM manufacturer (and those of the software developers, if any) are securely installed in the HSM. The first operation in the system boot-up is the integrity check of the middleware software. If it is the case, the middleware continues loading the remaining software elements, previously checking their integrity as well. It must be noted that this procedure ensures that, once the boot-up is finished, the system is in a *secure* status, that is, there are no compromised software elements and, moreover, the middleware is offering its regular security services [24].

Once the boot-up is finished, the system is able to operate regularly. For the focus of this work, this is translated into sending and receiving messages by the running applications, with other nodes such as RSUs or back-end servers. In order to send a message that requires some cryptographic operation (e.g. encryption, signature, hash), the application requests the secure I/O partition to perform the cryptographic operation. This request is redirected to the crypto software module, which interacts with the HSM to get the required result. It is sent back to the requesting application, which is now able to prepare the message. Afterwards, the application asks the secure I/O partition to send the message to the OBU for its transmission. All these interactions are performed through the middleware. The process in the reception is similar. Once a cryptographic operation is needed over an incoming message by the OBU, it is sent to the secure I/O partition. Based on the message type, this component decides which application is in charge of its management. The message is then sent to the appropriate application, which may require the interaction of the crypto software module (again through the secure I/O partition) in order to perform the cryptographic operation.

All the aforementioned considerations reveal that all components that are under the control of the middleware are trustworthy, in the sense that they operate correctly. Such components are highlighted in Figure 2.2. However, it must be noted that the HMI devices, the in-vehicle sensors and the OBU may be *physically* altered.

For the sake of brevity, the interaction with the Secure I/O partition and the Cryptographic software controller is omitted in the description of the mechanisms proposed in this thesis. Therefore, it is shown as a direct interaction between the SAE and the HSM.

2.3 Security issues in VANETs

This Section introduces the security requirements related to VANETs (Section 2.3.1) and the corresponding attacks (Section 2.3.2). Furthermore, given that a significant part of the data exchanged in a VANET is related to sensorial measurements, Section 2.3.3 presents their security issues. Particularly, given that steganography has been used to prove ownership or integrity of such data (by inserting some information within), previous approaches on this direction are reviewed. This particular technique is of relevance for this thesis as it enables embedding information within transmitted data, which will be the basis for the contribution C2 concerning the covert reporting of misbehaving vehicles.

2.3.1 Security requirements

Taking into account the different entities and data at stake, in this Section a catalogue of security requirements for each VANET setting is built. Although I2V and V2I were considered to be the same setting, they have different security requirements and so they have been distinguished here.

First of all, *entity identification* imposes that each participating entity should have a different and unique identifier. However, identification itself does not imply that the entity proves that it is its actual identity - this requirement is called entity authentication. Each of the application groups (enabled by the communication patterns previously introduced) has different needs regarding to these requirements.

V2V warning propagation needs identification to perform message routing and forwarding - identifiers are essential to build routing tables. *Sender authentication* is also needed for liability purposes. Imagine that a regular vehicle sends a notification as if it were a police patrol. It should be then needed to prove the identity of the emitting node. In group communications it is not required to identify or authenticate the communicating peers. The only need is to show that both participating entities have the required attributes to become group members - this is the attribute authentication requirement. In fact, this is the only communication pattern that needs this requirement. In beaconing, identification and authentication of the sender is needed. Nearby vehicles can then build a reliable neighbour table. Both requirements are also present in I2V warnings, where only messages sent by the infrastructure are credible. Infrastructure warnings are sent to all passing vehicles within an area, so identification or authentication of the receiver is not needed. On the contrary, V2I warnings also require the emitting vehicle to be identified and authenticated. In this way, only vehicles with a trustworthy identity will be able to send such messages.

Accomplishing the cited requirements should not imply less privacy. In fact, *privacy preservation* is critical for vehicles. In the vehicular context, privacy is achieved when two related goals are satisfied - *untraceability* and *unlinkability* [25]. The first property states that vehicle's actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, the second property establishes that it should be impossible for an unauthorized entity to link a vehicles identity with that of its driver/owner. However, this privacy protection should be removed when required by traffic authorities (i.e. for liability attribution). This requirement is present in all V2V communications. In fact, privacy should not get compromised even if different messages (no matter if under different communication patterns) are sent by the same vehicle. It does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes. In group communications it is not generally required, as the emitting node could be any of the group members. With respect to I2V and V2I warnings, non-repudiation of origin is needed, so wrong warning messages can be undoubtedly linked to the sending node. Non-repudiation of receipt is not currently needed, but it will be in the future. Currently, accident responsibility relies only on the human driver. However, in the future there are some envisioned applications that would automate partially the driving task. In such situation, not receiving a warning message could be critical for liability attribution.

Another important security requirement in vehicular communications is *confidentiality*, that is, to assure that messages will only be read by authorized parties. This requirement is present in group communications, in which only group members are allowed to read such information. Furthermore, some I2V/V2I warnings may be particular for a given vehicle, thus requiring a confidential communication.

The *availability* requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and mechanisms should save as much bandwidth and computational power as possible, while fulfilling these security requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also I2V ones.

Finally, related to the information itself, *data integrity* and *accuracy* must be assured. Both needs are globally referred as data trust. Data at stake should not be altered and, more importantly, it should be truthful. It also implies that received information is fresh (i.e. refers to the current state of the world). False or modified data should lead to potential crashes, bottlenecks and other traffic safety problems.

For this reason, data trust must be provided on all VANET communications.

2.3.2 Overview of attacks in VANETs

Once the security requirements have been established for VANETs, many attacks can be identified to compromise them [26]. In this Section we elaborate on these attacks, explaining how they can be performed and their potential consequences. For the sake of clarity, attacks have been classified depending on the main affected requirement.

Attacks on identification and authentication

There are two main attacks related to identification and authentication:

Impersonation. The attacker pretends to be another entity. It can be performed by stealing other entity's credential. As a consequence, some warnings sent to (or received by) a specific entity would be sent to (or received by) an undesired one. There exists a subtype of impersonation, called *false attribute possession*, in which the attacker tries to show the possession of an attribute (e.g. to be a member of an enterprise) to get some benefit. It could be performed if false credentials could be built, or if revoked credentials could be used normally. As a consequence, a regular vehicle could send messages claiming to be a police patrol, letting it to have a free way.

Sybil. The attacker uses different identities at the same time. In this way, a single vehicle could report the existence of a false bottleneck. As presented in the VANET model, TPMs mounted on vehicles can store sensitive information like identifiers. In this way, the Sybil threat is alleviated. However, security mechanisms must be designed to provide identification and authentication, thus protecting against impersonation attacks.

Attacks on privacy

Attacks on privacy over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle's circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

Identity revealing. Getting the owner's identity of a given vehicle could put its privacy at risk. Usually, a vehicle's owner is also its driver, so it would simplify getting personal data about that person.

Location tracking. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle's profile and, therefore, that of its driver. Mechanisms for facing both attacks are required in VANETs. They must satisfy the trade-off between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

Attacks on non-repudiation

The main threat related to non-repudiation is denying some action by some of the implicated entities. Non-repudiation can be circumvented if two or more entities share the same credentials. This attack is different from the impersonation attack described before - in this case, two or more entities collude to have a common credential. In this way, they get indistinguishable, so their actions can be repudiated. Credential issuance and management should be secured in VANETs to alleviate this threat. Although reliable storage has been assumed in vehicles (by their TPMs), having identical credentials in different vehicles should be avoided. Moreover, mechanisms that provide a proof of participation have to be also implemented.

Attacks on confidentiality

Eavesdropping is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

Attacks on availability

As any other communication network, availability in VANETs should be assured both in the communication channel and in participating nodes. A classification of these attacks, according to their target, is as follows:

Network Denial of Service (DoS). It overloads the communication channel or makes its use difficult (e.g. interferences). It could be performed by compromising enough RSUs, or by making a vehicle to broadcast infinite messages in a period of time. A particular case of network attack is *routing anomalies*, which could lead to a DoS. In this case, attackers do not participate correctly in message routing over the network. They drop all received messages (sinkhole attack) or just a few ones according with their interests (selfish behavior).

Computation DoS. It overloads the computation capabilities of a given vehicle. Forcing a vehicle to execute hard operations, or to store too much information, could lead to this attack.

Attacks on data trust

Data trust can be compromised in many different ways in VANETs. Inaccurate data calculation and sending affects message reliability, as they do not reflect the reality. This could be performed by manipulating in-vehicle sensors, or by altering the sent information. Imagine that a vehicle reports an accident in road E-7, while it really took place in E-9. Such information should compromise such messages' trust. Even worse, sending false warnings (e.g. the accident did not take place) would also affect the whole system reliability. In this way, mechanisms to protect against such inappropriate data should be put in practice in vehicular contexts.

2.3.3 Security over sensorial information: Steganography-based approaches

This Section gives a brief background on steganography and how it has been applied over sensorial data. For the sake of brevity, only the most basic notions on this issue are introduced herein. Interested readers may refer to [27].

Definition

Steganography is the science that studies the techniques to hide the existence of messages [28]. Steganography shall not be confused with cryptography, which main aim is to conceal the content of the message so only allowed parties are able to read it. On the contrary, steganography aims *to hide* the message itself.

The first informal description of steganography was given by Simmons as the prisoners problem [29]. Simmons described two prisoners (Alice and Bob) who want to plot an escape plan. As they are not in the same cell, they must communicate through a warden (Willie) that will analyse any communication between them. If Willie ever suspects that Alice and Bob are exchanging secret information he will put them into isolation cells and the escape plan will be frustrated. In this scenario, Alice and Bob will not be able to directly use cryptography as the unintelligible messages between them will raise suspicions on Willie. In order to achieve their goal, they should hide their messages into innocuous looking ones, so Willie will not be aware of the real meaning of those messages.

Elements of a steganographic system

The prisoners problem shows the different elements that take part in a steganographic communication (Figure 2.3).

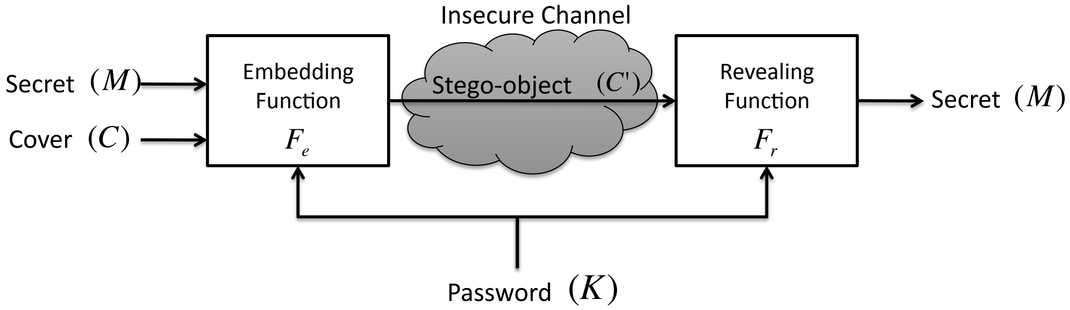


Figure 2.3: Elements of a steganographic system

Let M be the secret message to be covertly sent. Let C be the innocuous message (cover) used to embed the hidden information. Let K be a pre shared password known by both the sender and the recipient of the message. The embedding function, $F_e(M, C, K)$, takes as input the cover C, the secret message M and the password K and outputs a Stego-object C' which looks like the original cover. To improve the security of the embedded data, F_e usually encrypts the secret message before embedding it into the cover. The stego-object is sent to its recipient through an insecure channel that may be controlled by a warden. On reception, the revealing function $F_r(C', K)$ is applied. F_r takes as input the stego-object C' and the pre-shared password K and outputs the secret message M.

Desirable properties

The main goal of steganography is to build embedding functions that allow participants to embed practical amounts of information into covers in such a way that an attacker cannot detect the presence of hidden information [30]. To produce undetectable stego-objects, there should not be statistical differences between the set of all possible covers C and the set of generated stego objects C'. Thus, it should not be possible to detect whether an object has embedded information or not without the knowledge of the key. In this regard, true randomness found in covers is the best carrier for steganographic information [31]. Replacing this with encrypted information would not change the statistical properties of the cover, given that the encryption result is assumed to be random.

Apart from the effectiveness of the mechanism, it is desirable that it offers the maximum capacity to embed information while remaining undetected. Furthermore, two desirable properties are the resistance against passive attacks (e.g. eavesdropping) as well as against active ones (e.g. data alteration).

Previous approaches

Steganography and other information hiding techniques have been used to embed some information within sensor generated data. These approaches are usually devoted to prove ownership or integrity of sensor-generated data.

The work in [32] proposed a system that was able to watermark raw sensor data in real time by modifying sensor constraints such as its position, resolution and data gathering frequency. Similarly, Zhang et al. use watermarking techniques to authenticate sensor-generated data [33]. Sensor data is transformed in an image in which each pixel intensity is related to the sensor measurement. Sensor images are then watermarked. Transmission of gathered sensor data uses a lossy compression algorithm, producing slight differences on gathered data at the other end of the communication. Checking the embedded watermark allows to verify if produced differences are acceptable.

A more general approach to sensor data watermarking was proposed in [34]. The proposed system requires, besides the numeric set to be watermarked, the definition of *usability metrics* for the numerical set. The set is divided into non overlapping subsets. For each subset, the algorithm tries to embed a bit of the watermark without exceeding the restrictions imposed by the usability metrics. Sets that can not be altered without exceeding the usability metrics are ignored.

Despite the relevance of sensorial data in VANETs, to the best to this thesis author's knowledge there are not previous contributions related to the application of steganography for the particular sensor information at stake in these networks.

Chapter 3

Enforcement process. Technical and legal issues

This chapter introduces the technical and legal issues of the road traffic enforcement process, which are the context of this thesis. First, a description on the current process and its implementing systems is given in Section 3.1. After this general view of the process, the following Sections focus on the specific issues related to the contributions of this thesis. Particularly, Section 3.2 introduces the electronic notification and its legal framework and Section 3.3 describes the electronic evidence. Section 3.4 is devoted to identify the main problems of the road traffic enforcement process. Finally, the parts of the European ITS architecture providing support for law enforcement are described in Section 3.5. It should be noted that the European ITS architecture seems to be the most outstanding contribution for the context of this thesis, as it is intended to be the general framework for ITS systems.

3.1 Current model and implementing systems

This Section describes the considered enforcement model, which is the result of the VERA2 (Video Enforcement for Road Authorities 2) project. Such model is composed by a set of flowcharts and a data dictionary. In this Section, only the speeding enforcement flowchart will be presented, as it is in the scope of this thesis. Furthermore, the Spanish and French systems that implement the enforcement in these countries are introduced.

3.1.1 VERA2 model

The enforcement process starts when the illegal action is detected and finishes when the punishment has been established. In between, several steps may take place. Countries like Spain group them into four phases - starting, preliminary investigation, resolution and appealling [35]. For the sake of clarity, such division will be employed to describe the process. Figures 3.1 and 3.2 show the different steps that happen during the process, grouped in the aforementioned phases.

Starting

The enforcement process starts with the detection of the illegal action. It may be detected either by the Authority or by any person that knows about the offence. Supporting evidences are collected and sent to the Authority for evaluation. If the Authority considers the action as an offence, a fine notification is issued and sent to the vehicle owner. In order to retrieve the owner information, the vehicle license plate is analysed. In case that it is a foreign vehicle, its corresponding national database or the EUCARIS one (EUropean CAR and driving licence Information System[1]) is contacted.

Preliminary investigation

There are two actions that may be performed by the offender in this phase. First, the owner[2] can nominate another person as the offending driver. Then, the notification is sent to this person. It must be noted that these notifications may be ignored by its receiver and, in some cases, re-sending them is allowed. In case that the notification is finally not ignored, the second action is to contest the fine. As a result, if the fine is cancelled, this decision is sent to the offender.

[1] https://www.eucaris.net/

[2] The vehicle's owner is the person who is legally responsible for the vehicle. It is also commonly referred to as *vehicle keeper*. Both concepts will be used interchangeably throughout this thesis.

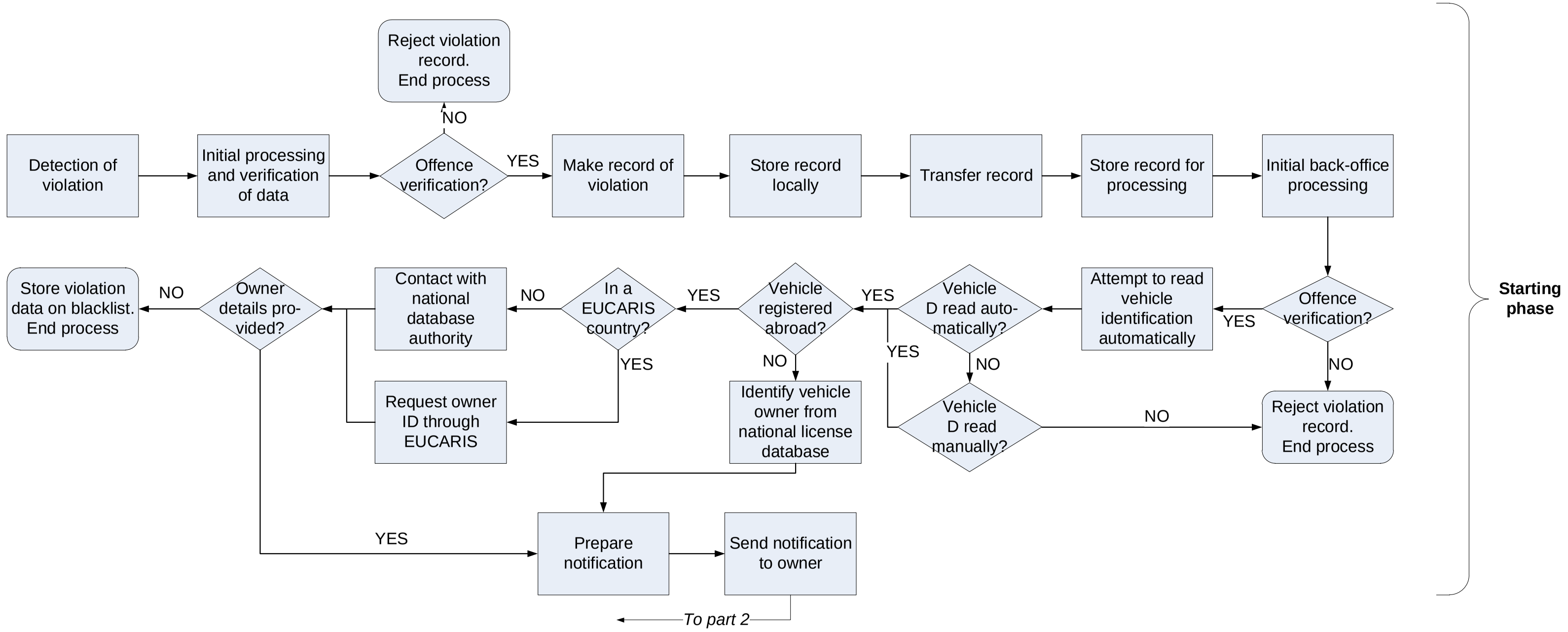

Reject violation record. End process
NO
Detection of violation
Initial processing and verification of data
Offence verification?
YES
Make record of violation
Store record locally
Transfer record
Store record for processing
Initial back-office processing
Starting phase
Store violation data on blacklist. End process
NO
Owner details provided?
Contact with national database authority
NO
In a EUCARIS country?
YES
Vehicle registered abroad?
YES
Vehicle D read automatically?
Attempt to read vehicle identification automatically
YES
Offence verification?
YES
NO
NO
YES
NO
Request owner ID through EUCARIS
Identify vehicle owner from national license database
Vehicle D read manually?
NO
Reject violation record. End process
YES
Prepare notification
Send notification to owner
To part 2

Figure 3.1: VERA2 process model, based on the material provided at [10]. Starting phase.

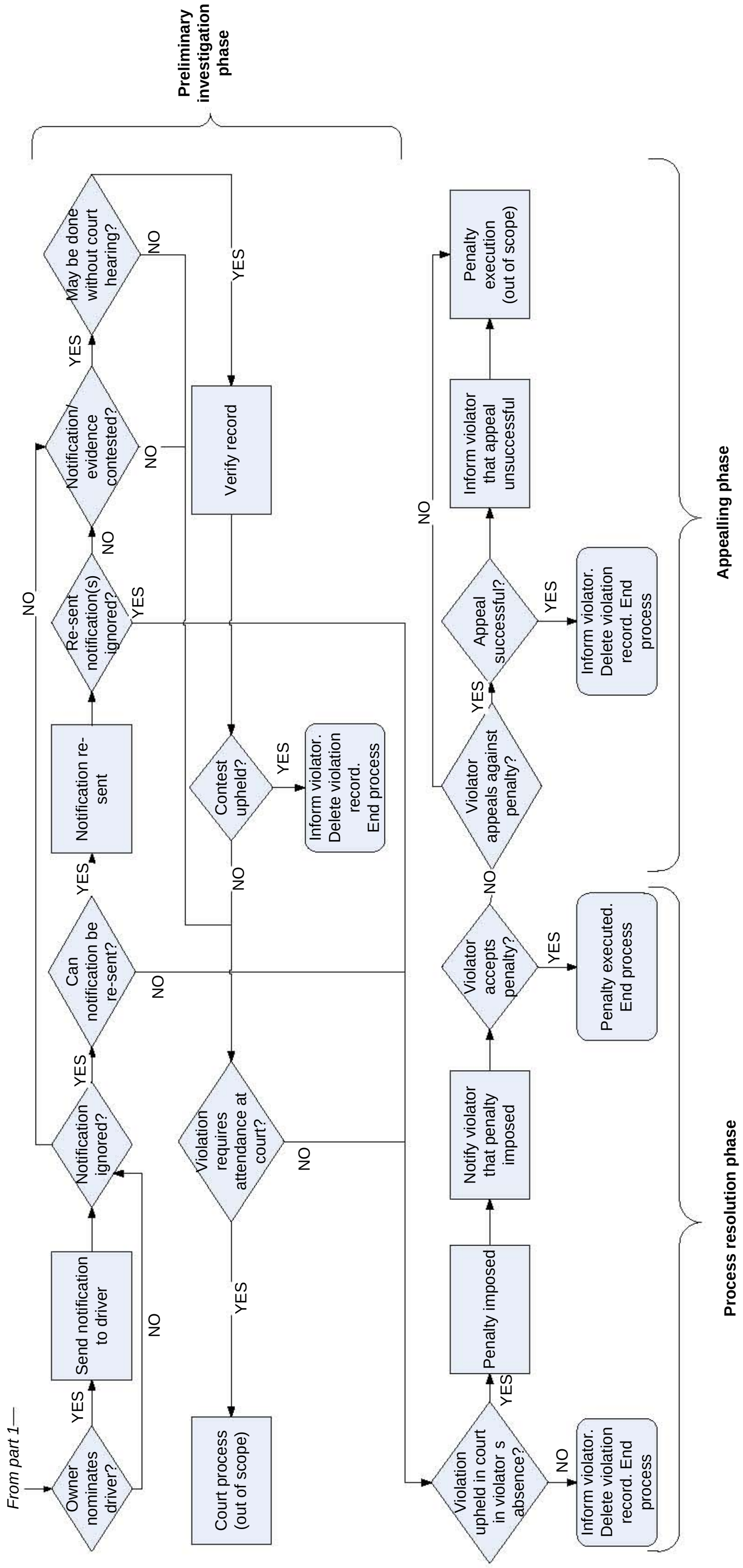

Preliminary investigation phase
From part 1
Owner nominates driver?
YES
NO
Send notification to driver
Notification ignored?
YES
NO
Can notification be re-sent?
YES
NO
Notification re-sent
Re-sent notification(s) ignored?
YES
NO
Notification/ evidence contested?
NO
YES
May be done without court hearing?
NO
YES
Verify record
Contest upheld?
YES
Inform violator. Delete violation record. End process
NO
Violation requires attendance at court?
YES
NO
Court process (out of scope)
Violation upheld in court in violator s absence?
YES
NO
Inform violator. Delete violation record. End process
Penalty imposed
Notify violator that penalty imposed
Violator accepts penalty?
YES
Penalty executed. End process
NO
Violator appeals against penalty?
YES
NO
Appeal successful?
YES
Inform violator. Delete violation record. End process
Inform violator that appeal unsuccessful
Penalty execution (out of scope)
Process resolution phase
Appealing phase

Figure 3.2: VERA2 process model, based on the material provided at [10]. Remaining phases of the enforcement process.

Resolution

If the previous phase has not cancelled the fine, an independent revision of the whole process is conducted. It verifies whether the process development is law respectful and thus if the offence is uphold. In any case, the revision result is notified to the offender.

Appealling

After receiving such notification, if the penalty is imposed the offender may accept or appeal it. In the latter case, she creates a document expressing the reasons to proceed, and sends it to the Authority for evaluation. The result of this process is notified to the sender. In case that the appeal has not removed the fine, the penalty is executed.

3.1.2 Overview of current enforcement systems. Case studies: Spanish ESTRADA and French CSA

Most enforcement systems in developed countries have some of their steps automatised. However, such automated devices are usually only employed in the Starting phase. Systems like the Spanish ESTRADA [36] or the French CSA [37] are good representatives of this enforcement trend. Both systems are composed by fixed and mobile speed cameras that are connected to a central processing office. Here, the license plate is extracted from the pictures taken, and the vehicle holder is identified by retrieving this information from the official register. The fine notification is prepared to be sent by post to the vehicle holder. All these steps are performed automatically.

Beyond this point, there are some slight differences between both systems. In the Spanish case, a recent revision of the traffic law has allowed sending this notification by electronic mail [6]. The notification receiver may also receive a short text message in her mobile phone indicating that such notification has been sent. The French case does not provide with this option. Moreover, the French system requires the vehicle holder to pay the fine prior to identifying the real driver in the Preliminary investigation phase [38].

3.2 Spanish legal framework on electronic notifications

This Section describes the legal framework regarding the requirements on the notification system, the notification process and the contents of an offence notification.

A significant part of the legal regulation of the electronic notification is focused on establishing the guarantees that must be provided to ensure the notification validity. Thus, Section 3.2.1 describes the general mechanisms and their requirements. Section 3.2.2 describes the contents of a road traffic notification.

3.2.1 Mechanisms for electronic notification. Requirements

The Royal Decree 1671/2009 establishes four ways in which the electronic notification may be performed, namely (1) the use of a specific (authorized, 'habilitada') electronic address, (2) the use of a mail system which attests the message reception, (3) the access to the electronic site of the notifying party, or (4) any other mechanism that attests the reception of the message within the time interval and satisfies its own regulatory issues [39].

Even if the notification mechanism proposed in this thesis (see Chapter 6) lays into the last type (thus being subject to its own regulation), it is convenient to analyze the requirements imposed to the remaining types in order to predict which ones will be applied to this new mechanism in the future. It should be noted that all mechanisms should protect the citizens' rights to the same extent, no matter how they internally work. Concerning the authorized electronic address, it must attest the date and time of the availability of the notification. The same information must be attested for the moment in which the notification is accessed. It must provide a permanent access and there should be an authentication mechanism that ensures the identity of the accessing person as well as its exclusive access. Additionally, the Legal Order PRE-878/2010 imposes a set of additional requirements for those entities that do not have their own regulatory framework [40]. Thus, it imposes the data confidentiality, the use of physical security measures, the protection of storage devices and the temporal attestation based on the data provided by the Spanish Real Observatorio de la Armada.

With respect to the electronic mail, a receipt must be issued in an automatic and unavoidable way. It must be issued once the notification content is accessed by the receiver. Regarding the mechanism based on the electronic access to the notifier site, the user must be authenticated and, prior to accessing to the content, a warning message must be displayed. Once such warning is accepted, the system must record the date and time of this action.

Road traffic electronic notifications. Spanish Dirección Electrónica Vial (DEV)

The Spanish Law 18/2009 defines one specific type of authorized electronic address called Dirección Electrónica Vial (DEV) [6]. Thanks to the DEV, the *physical home becomes a virtual home*, as the place to receive notifications[3]. Such mechanism aims to ensure that the citizen is always aware of his/her legal procedures[4].

Once a notification has been received, the receiver may accept, reject or ignore it. In order to avoid the process to get stopped in this point, if the notification is not accepted or rejected in ten days, it will be considered as rejected. This interval will be cancelled if there is a way to prove that it was not possible to access to the notification[5].

[3] Translated from the Spanish: "El tradicional concepto de domicilio físico se transforma ahora en domicilio virtual".

[4] Derived from the Spanish: "Las notificaciones mediante boletines oficiales (...) no ofrecen garantía material alguna al ciudadano de que tenga siempre conocimiento de los procedimientos que contra él se dirigen. En estas circunstancias se crea la Dirección Electrónica Vial (DEV)".

[5] Translated from the Spanish: "Si existiendo constancia de la recepción de la notificación en la Dirección Electrónica Vial, transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que aquélla ha sido rechazada, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.".

The legal requirements on the DEV are very similar to those applied to the authorized address. Particularly, the date and time of the notification availability must be attested, as well as the moment of the access to the notification.

3.2.2 Road traffic notification contents

Based on Law 18/2009, road traffic notifications must contain the following five sets of data [6]:

- Offender: identification of the vehicle, identification of the offender (if known), address to perform notifications (or DEV, if the offender has enabled it).
- Offence: offence description (place, date and time), violation purportedly committed.
- Reporting entity: name and address of the reporting entity (or professional identification, in case of road traffic agents).
- Punishment: Authority enabled to set the punishment and legal reference of such designation. Punishment description and demerit points that are at stake.
- Future actions: Amount of payment already satisfied, legal consequences of partial payment. Legal explanation on the process, place and time interval to introduce allegations and counterevidences.

3.3 Electronic evidence. Description and precedents in ITS-related environments

Electronic evidences are the main mechanism to build attestations in the electronic context. In the road traffic enforcement process, they may serve to attest some driving behavior.

Electronic evidences have suffered a great evolution in the recent years, as a consequence of the generalization of computer forensics techniques. This Section describes electronic evidences (Section 3.3.1), their associated management cycle (Section 3.3.2) and the previous works that have focused on applying these concepts in vehicular environments (Section 3.3.3).

3.3.1 Definition and principles

According to the Merriam-Webster dictionary[6], an evidence is defined as *something legally submitted to a tribunal to ascertain the truth of a matter.* In order to capture the specific issues of the electronic world, a refined version has been built for electronic evidences. Thus, it has been defined as *any trace that has been created by, or stored in, a computational system, that may be used as a proof in a legal process*[7] [41].

At the light of the previous definitions, electronic evidences are intended to be submitted for their consideration in Courts. It is a matter of the Authority in force (e.g. judge, administrative supervisor, etc.) to evaluate its relevance and impact within the process at stake. Prior to such evaluation, evidences must satisfy some principles in order to be accepted as a legal proof. Although these principles may vary between different countries, four generic ones have been identified [42]:

- Authenticity and reliability. The evidence must be genuine and must contain reliable data.

- Completeness, containing all the data required to support the claim or hypothesis at stake.

- Law conformance, remarkably ensuring that it has been obtained without threatening other rights.

[6] http://www.merriam-webster.com/dictionary/

[7] Translated from the Spanish: "Cualquier registro generado por, o almacenado en, un sistema computacional que puede ser utilizado como prueba en un proceso legal".

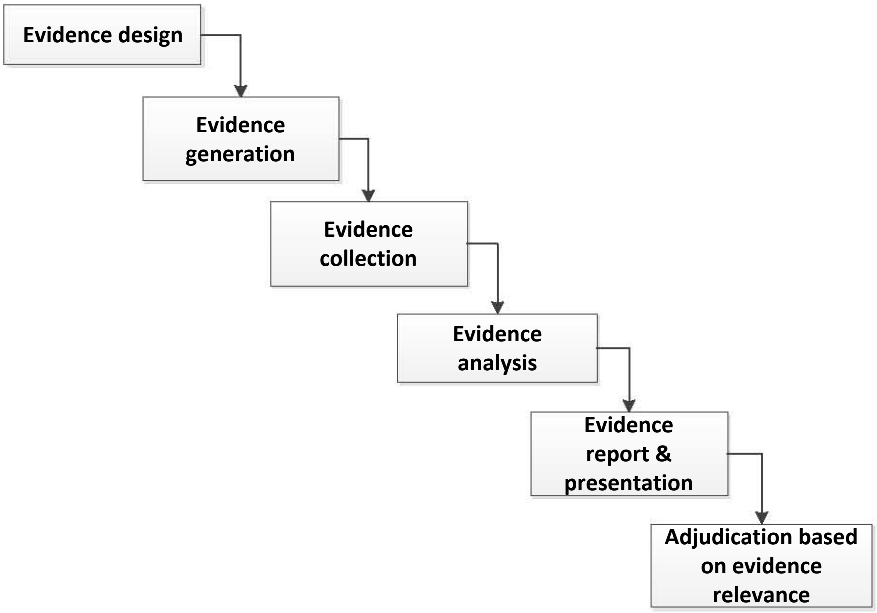

Evidence design
Evidence generation
Evidence collection
Evidence analysis
Evidence report & presentation
Adjudication based on evidence relevance

Figure 3.3: Evidence management process as defined by Cano [41]

3.3.2 Management cycle

In order to ensure that the evidence will respect the aforementioned principles, a management cycle is required (see Figure 3.3). Such cycle should preserve the evidence during the whole process, from the moment in which it is obtained and until it is used in Courts. Despite the fact that an international, worldwide standard does not exist, an essential sequence of steps have been identified by Cano [41].

The first step involves designing the evidence, that is, setting its format and the information that should be contained in it. The second phase creates the evidence, whereas the third step collects it. In the fourth step, it is analysed to establish whether it is suitable or not to support (or refute) a given hypothesis. If it is the case, the evidence is transferred to the adjudicator (i.e. the entity that will take a decision to solve the current controversy). In the last step, the evaluation by the adjudicator is performed.

3.3.3 Precedents in vehicular networks

To the best of the author's knowledge, there are little scientific contributions on evidence generation in these scenarios. The most representative ones are related to accident reconstruction. In [43], Hardware Security Modules (HSMs) are employed to register all the events produced by the own car. Once the crash has happened, involved vehicles send informative beacons to the surrounding vehicles to alert them on the situation. Furthermore, HSMs of crashed vehicles become a black box.

The aforementioned existence of black boxes in vehicles have been generalized in a family of devices called Motor Vehicle Event Data Recorders (MVEDR). These devices, normalized under IEEE 1616 standard, are intended to register the own vehicle's sensor measurements [22]. The main problem of these devices is that they only ensure that the stored data is securely managed. However, before arriving to this device the information is created by a sensor and transmitted through an in-vehicle communication network. Unless they are properly secured, both the sensor and the communication network may be compromised. In such a situation, evidences based on data stored in MVEDRs may be called into question.

Evidence generation is also present in the security framework presented by Lin *et al.* [44]. Their focus is on building a secure and private communication protocol that ensures efficient traceability when needed. Thus, they consider the signed traffic messages sent by one entity as an evidence. Once an incident happens, two Authority-related entities (Tracing Manager and Membership Manager) collaborate to reveal the signer's identity based on the aforementioned evidence.

3.4 Problems of the enforcement process

Based on [4][45], current automated systems face three main problems. Each one is introduced in the following subsections.

3.4.1 Problem 1. Lack of a reliable and immediate offender identification

Current automated systems have a lack of reliable offender identification. Automated devices such as cameras have to combine their effectiveness with the drivers right of privacy protection. Thus, graphic evidences (i.e. pictures or videos) usually only show the vehicle's rear [46].

To solve this liability-privacy tradeoff, the fine is firstly referred to the vehicle's owner who identifies the actual driver (as explained in Section 3.1.1). This method has two main drawbacks. First, the process is delayed, as the owner has to perform the mentioned identification. For example, Spanish legislation enables up to 15 days for this purpose, added to the time to deliver the notification. Second, it can lead to identification frauds. This is especially relevant in those countries where sanctions can have consequences over the driving licence (i.e. demerit points, license withdrawal).

Using pictures or videos to identify the vehicle has another drawback. The effectiveness of current Automatic Number Plate Recognition (ANPR) systems is not complete, but around 90 per cent [47]. Moreover, singularities of the number plates in different countries make difficult to identify foreign offending vehicles.

3.4.2 Problem 2. Notification delays

Notifications introduce a delay in the process composed by three factors: the time to prepare the notification ($t_{prep.notif}$), to send it ($t_{send.notif}$) and to access to it by the receiver ($t_{delay.access}$). Recent estimations in Spain showed that such delay was 45 days for postal notifications and 12 days for electronic ones [11]. Manual notifications are usually performed in some minutes, as they only require to fill up a form. Even if such notifications are the most immediate ones, they may only be applied to a short proportion of offences due to the limitation of human resources. Therefore, for most offences its notification arrives after several days, which decreases its educational purpose [4].

3.4.3 Problem 3. Unfairness: Incomplete offence descriptions and lack of witnesses

Nowadays, automated surveillance devices (such as cameras) or even police agents are the main data sources employed to describe the offence. Such data sources observe the situation from a single point *outside* the vehicle. However, sensorial errors (for devices) as well as perception limitations or even psychological factors (for persons) may offer inaccurate offence descriptions, thus leading to unfair punishments. This situation may not be countered by drivers, as usually there are no witnesses to support their claims [45].

3.5 Support for law enforcement by the European ITS architecture

The European architecture on ITS provides support for the enforcement process [48]. This support is focused on the initial evidence collection and transfer to the law enforcement agency. Figure 3.4 shows the Data Flow Diagram (DFD) that describes the data flows and operations related to this process. First, the Detect Fraud or Violation determines whether a given action is against the rules. For this purpose, it is assisted by the Identify Violator function, which returns the identification of the vehicle involved and that of the person who is responsible for such vehicle. It should be noted that this function takes into account the chance of retrieving data from the on-board vehicular equipment. Thus, it considers requesting the Driver for some data produced by the on-board vehicular equipment, such as speed, pollution, driving schedule, etc. Furthermore, it also uses the vehicular identification provided by such devices.

Based on the initial determination of the type of offence, the vehicle identification and that of its responsible person, the Process Fraud and Violation Notifications function creates the prosecution file. Such file contains all the data required to prosecute a violator – description of the offence (date, place, description, means used to detect it, available proofs), of the offender (vehicle identification, owner/driver identification, previous offences) and the consequences of this action.

Once the file is built, it is sent to the Law Enforcement Agency to start the prosecution process. Therefore, the way in which such file is made available to the affected person, as well as the rest of the enforcement process (allegations, further investigations, etc.) is out of the scope of this architecture.

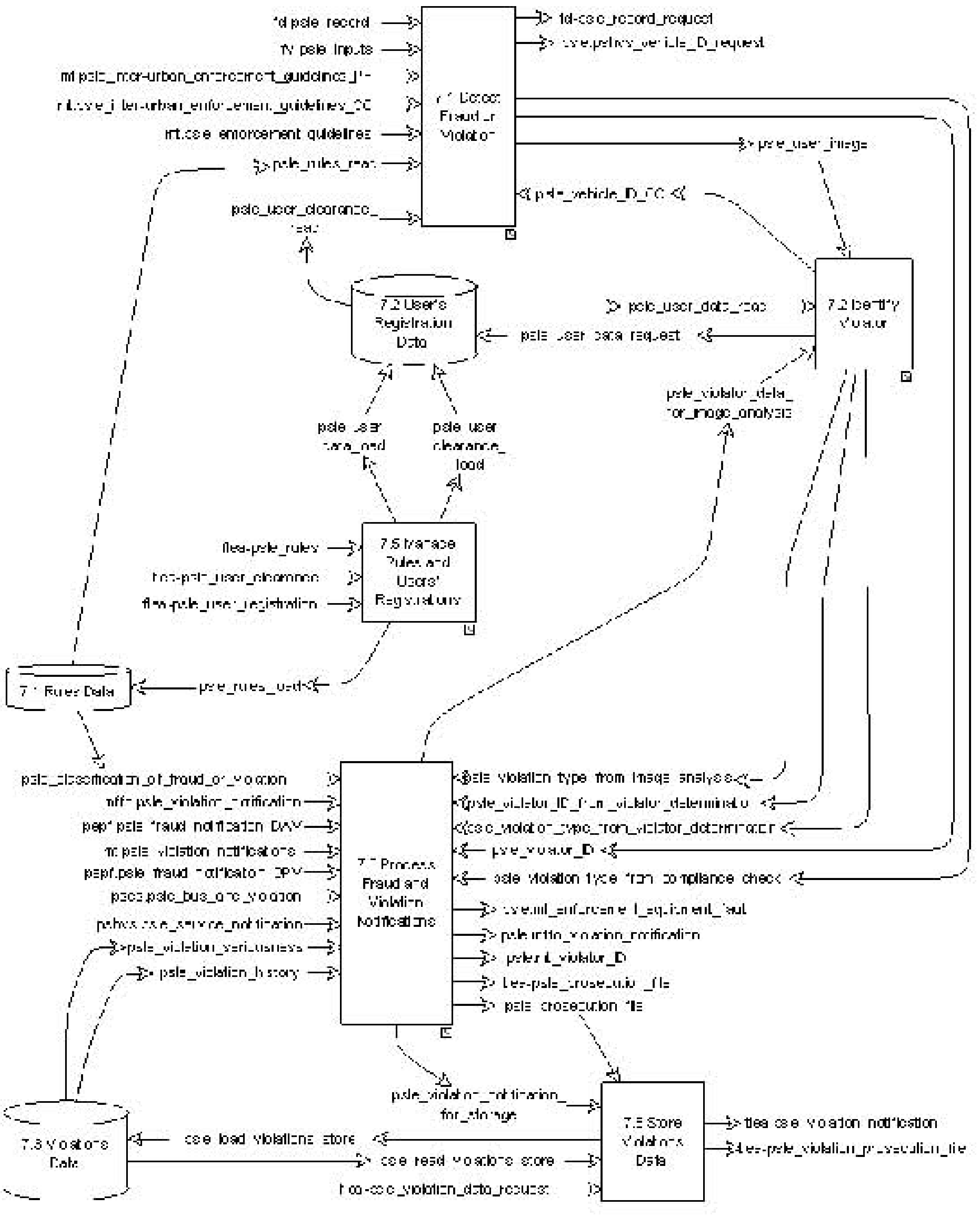

fd.pele_record
fv.pele_inputs
mf.pele_inter-urban_enforcement_guidelines_IM
mf.pele_inter-urban_enforcement_guidelines_CC
mf.pele_enforcement_guidelines
pele_rules_read
pele_user_clearance_read
7.1 Detect Fraud or Violation
fd-pele_record_request
pele.petrol_vehicle_ID_request
pele_user_image
pele_vehicle_ID_CC
7.2 User's Registration Data
pele_user_data_read
pele_user_data_request
7.2 Identify Violator
pele_violator_data_for_image_analysis
pele_user_data_load
pele_user_clearance_load
flea-pele_rules
flea-pele_user_clearance
flea-pele_user_registration
7.5 Manage Rules and Users' Registrations
7.4 Rules Data
pele_rules_used
pele_classification_of_fraud_or_violation
mff.pele_violation_notification
pepf.pele_fraud_notification_DAV
mf.pele_violation_notifications
pepf.pele_fraud_notification_DPV
pepd.pele_bus_lane_violation
pehvs.pele_service_notification
pele_violation_seriousness
pele_violation_history
7.7 Process Fraud and Violation Notifications
pele_violation_type_from_image_analysis
pele_violator_ID_from_violator_determination
pele_violation_type_from_violator_determination
pele_violator_ID
pele_violation_type_from_compliance_check
pele.mf_enforcement_equipment_fault
pele.mf_violation_notification
pele.mf_violator_ID
flea-pele_prosecution_file
pele_prosecution_file
pele_violation_notification_for_storage
7.6 Violations Data
pele_load_violations_store
pele_read_violations_store
flea-pele_violation_data_request
7.8 Store Violations Data
flea.pele_violation_notification
flea-pele_violation_prosecution_file

Figure 3.4: European ITS architecture – ‘Provide support for law enforcement’ DFD [49]

Part III

Proposal

Chapter 4

Enhanced road traffic administrative enforcement process model for speeding offences and ITS realization

The VERA2 project provided an enforcement process model, particularly applied to speeding offences, that allows understanding its main steps. Nevertheless, this model is not enough to determine which ITS-related technologies are more suitable for this context, or their specific scope.

This Chapter introduces an enhanced model, based on the VERA2 one. It is focused on road traffic administrative offences caused by speeding. It complements the previous one by the identification of enforcement entities, stakeholders, data structures and interchanges. The data security and privacy considerations are also analysed. It is also identified the way in which ITS technologies may be applied in this context to contribute on the current problems of enforcement systems.

In order to perform the aforementioned enhancements, the system that realizes the enforcement process is considered. Section 4.1 presents the methodology employed to derive the enhancements. Section 4.2 describes the refinements made over the VERA2 process model to make it suitable to represent current enforcement practices. For this purpose, the Spanish case has been considered. Section 4.3 introduces the stakeholders that interact with the system to establish the appropriate fine. The legislation establishes several data structures to be present at each part of the process. Section 4.4 presents such data structures, which will be managed by enforcement entities (described in Section 4.5). The main data interchanges that happen during the process are depicted in Figure 4.1, whereas Appendix C specifies all of them in detail. Section 4.6 discusses the arising data security and privacy issues.

The selection of ITS technologies that may be applied to contribute on the identified enforcement problems (recall Section 3.4), as well as the parts of the proposed model affected by such integration, is presented in Section 4.7.

4.1 Methodology

In order to identify the proposed enhancements, two sources of information have been analysed: the VERA2 flowchart [10] and the Spanish traffic law [6]. As a result, some refinements over the VERA2 flowchart have been introduced. Afterwards, the flowchart steps have been grouped whenever they form a conceptual set of operations that may be addressed by an enforcement entity. Each of these groups (and thus, enforcement entities) has been given a name, leading to an initial set of entities.

The flowchart does not detail the stakeholders that participate in each step in the process. For this purpose, the Spanish traffic law has been analysed to extract this information. These stakeholders have enabled a classification of the aforementioned enforcement entities based on the relationships between such entities and the stakeholders (see Figure 4.1).

Finally, the legislation has also been analysed to determine the data at stake in each enforcement entity, along with their data interchanges. The data security and privacy needs have also been identified. A new block of enforcement entities was identified to store these data.

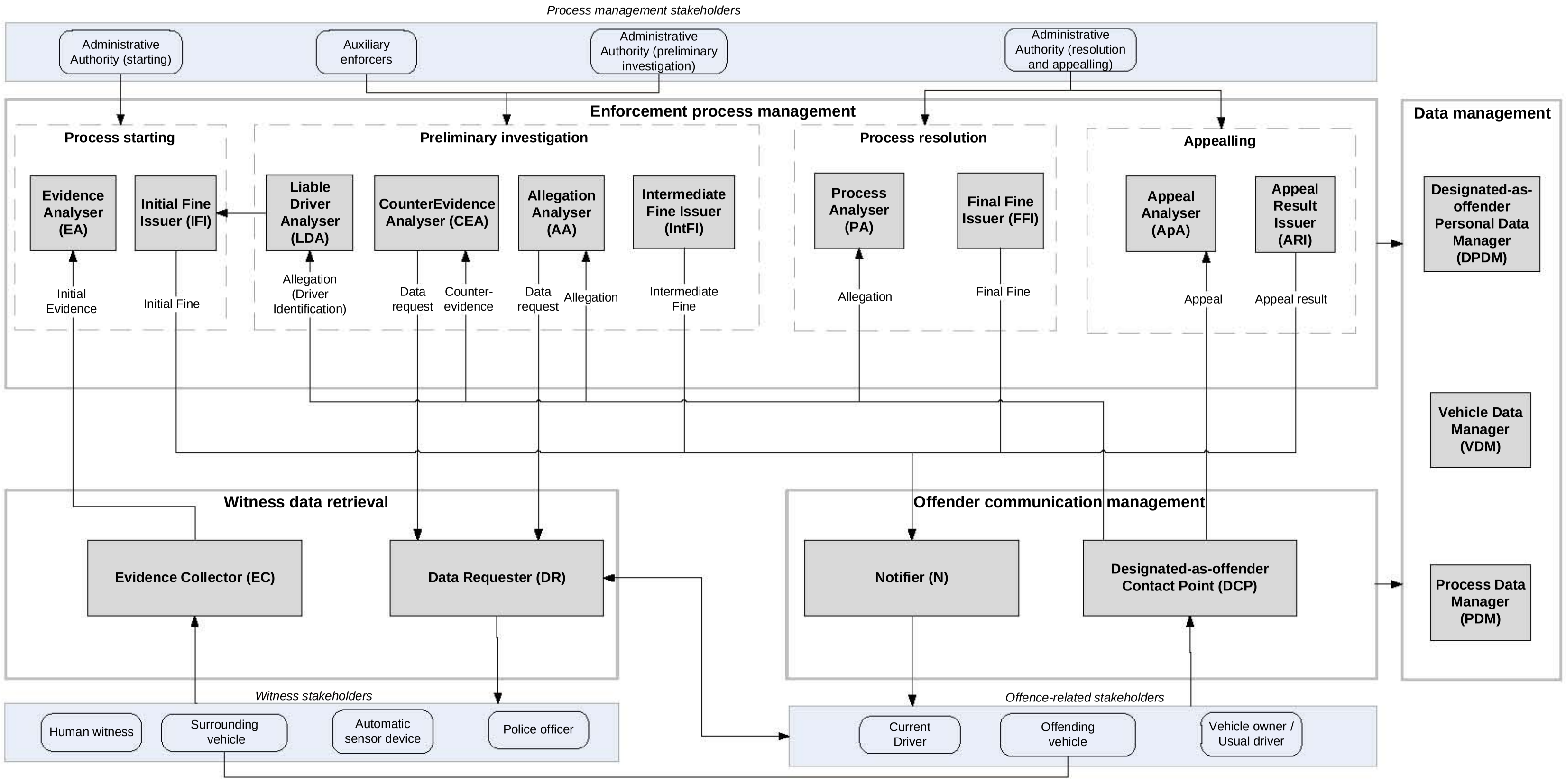

Process management stakeholders
Administrative Authority (starting)
Auxiliary enforcers
Administrative Authority (preliminary investigation)
Administrative Authority (resolution and appealling)
Enforcement process management
Process starting
Evidence Analyser (EA)
Initial Fine Issuer (IFI)
Initial Evidence
Initial Fine
Preliminary investigation
Liable Driver Analyser (LDA)
CounterEvidence Analyser (CEA)
Allegation Analyser (AA)
Intermediate Fine Issuer (IntFI)
Allegation (Driver Identification)
Data request
Counter-evidence
Data request
Allegation
Intermediate Fine
Process resolution
Process Analyser (PA)
Final Fine Issuer (FFI)
Allegation
Final Fine
Appealling
Appeal Analyser (ApA)
Appeal Result Issuer (ARI)
Appeal
Appeal result
Data management
Designated-as-offender Personal Data Manager (DPDM)
Vehicle Data Manager (VDM)
Process Data Manager (PDM)
Witness data retrieval
Evidence Collector (EC)
Data Requester (DR)
Offender communication management
Notifier (N)
Designated-as-offender Contact Point (DCP)
Witness stakeholders
Human witness
Surrounding vehicle
Automatic sensor device
Police officer
Offence-related stakeholders
Current Driver
Offending vehicle
Vehicle owner / Usual driver

Figure 4.1: Proposed enforcement system model

4.2 Refinements over the VERA2 process model

Four refinements are performed over the VERA2 process model. The first one aims to extend it to enforcement actions performed by police patrols, instead of only considering those registered by automated devices. Thus, the person identified as the offender (called *designated-as-offender* role, from now on) in the Starting phase may be not only the owner, but also the driver. Related to this point, the second refinement is that the legislation enables the owner to nominate another person as the usual driver. Therefore, she will receive the fine notifications at first, instead of the owner.

The third refinement is to specify the ways to contest the fine in the Preliminary investigation. Thus, there may be allegations and counterevidences. Allegations enable to have another view of the offence context, trying to decrease its severity. For example, medical emergencies may be considered as an alleviating factor for speeding. Regarding counterevidences, they are a piece of verifiable data describing the facts. As an example, a counterevidence could show that the vehicle speedometer did not reach that illegal speed. It may be built by the Authority after proposal from the offender or by its own initiative. For example, it may consist on checking whether the radar was properly calibrated.

The fourth refinement is related to the notification of the Intermediate fine (data structure described in Section 4.4). Such notification happens only once the fine has been contested and this action has not been upheld because of data or facts unknown to the offender. Moreover, only in this case the offender is enabled to defend herself by sending new allegations at the beginning of the Resolution phase.

4.3 Stakeholders

There are three groups of stakeholders in this process. The first one contains the participants related to the process management (see Figure 4.1, upper part). These are the administrative Authorities and the auxiliary law enforcers that support their work.

The second group (see Figure 4.1, lower left corner) contains the participants that have been witnesses of the offence, but are not the offender. According to the Spanish law, three types of witnesses may report an offence – persons, automated sensor devices or police officers [6]. Moreover, technically enabled vehicles could also become electronic witnesses.

The third group (see Figure 4.1, lower right corner) is composed by the entities directly related to the offence. Apart from the offending vehicle, it may be any entity that plays the designated-as-offender role (recall Section 4.2).

4.4 Data at stake

In this Section the data structures involved in the enforcement process are described (see Table 4.1), detailing their composing data elements based on the Spanish legislation [6]. For the sake of uniformity, the catalogue of information elements provided by the VERA2 dictionary is used when possible [10]. In Table 4.1, the element identifiers from that dictionary are marked in parenthesis (where *n/a* indicates that this data item is not in the dictionary).

In the Starting phase, two structures exist - the initial evidence and the initial fine. The *initial evidence* is the first description of the violation, whereas the *initial fine* is the first evaluation of the aforementioned violation conducted by the Authority.

Phase	Data structure	Information elements
Starting	Initial evidence	Vehicle data: identifier (e.g. number plate (65004)), make and model (65007,65008), type (65005). Offender data, if known: name (200, 201), postal address (218-222), identifier type and number (216, 217), driving licence type (n/a). Offence description: speed limit (65101), recorded speed (65102,65103), place (304-310) and time (311-313). Witness data, which may be one of: camera reference number (65001), recording device (65104,65105), person name (200, 201) and postal address (218-222), or police officer identifier (n/a).
	Initial fine	Initial evidence, Infraction data: infringed rule (300, 301, 314, 315), fine amount (700-703), demerit points cost (n/a). Authority issuing the fine: name and identifier (101,102), legal basis that enables the Authority (n/a). Legal process reference: identification number (505), date and time (n/a). Payment: amount already paid and remaining amount (704-706), consequences of partial payment (n/a). Period and procedure for allegations and counterevidences (n/a). Offender postal address (218-222).
Prelim. invest.	Allegation	Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Legal process reference: identification number (505). Vehicle data: number plate (65004), make and model (65007,65008). Allegation: alleged element(s) (n/a), motivation (n/a), allegation time (n/a) and place (n/a). Receiving Authority: name and identifier (101,102).
	Counterevidence	Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Legal process reference: identification number (505). Vehicle data: number plate (65004), make and model (65007,65008). Evidence data, which may be in form of: Testimony: person name (n/a) and postal address (n/a), testimony content (n/a). Graphical proof: picture or video (n/a). Probatory element: content (n/a). Counterevidence time (n/a) and place (n/a). Receiving Authority: name and identifier (101,102).
	Intermediate fine	Authority issuing the fine: name and identifier (101,102), legal basis that enables the Authority (n/a). Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Vehicle data: number plate (65004), make and model (65007,65008). Legal process reference: identification number (505). Considered facts: description (n/a), relevance (n/a). Proposed fine revised amount (n/a). Date and time (n/a). Period and procedure for allegations (n/a).

Table 4.1: Data structures on each process phase

Phase	**Data structure**	**Information elements**
Resolution	Allegation	Same contents as in the Preliminary investigation
	Final fine	Authority issuing the fine: name and identifier (101,102), legal basis that enables the Authority (n/a). Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Vehicle data: number plate (65004), make and model (65007,65008). Legal process reference: identification number (505). Considered facts: description (n/a), relevance (n/a). Definitive infraction data: infringed rule (300, 301, 314, 315), fine amount (700-703), demerit points cost (n/a). Payment issues: amount already paid and remaining amount (704-706), legal consequences of partial payment (n/a). Legal period and procedure to present appeals (n/a). Date and time (n/a).
Appealling	Appeal	Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Legal process reference: identification number (505). Appealling content: appealed elements (n/a), motivation (n/a). Receiving Authority: name and identifier (101,102). Date and time (n/a).
	Appeal result	Offender data: name (200, 201), postal address (218-222), identifier type and number (216, 217). Legal process reference: identification number (505). Resolution content: appeal result (n/a), motivation (n/a). Issuing Authority: name and identifier (101,102), legal basis that enables the Authority (n/a). Legal provision on the potential actions by the offender (n/a). Date and time (n/a).

Table 4.2: Data structures on each process phase (cont)

There are three data structures in the Preliminary investigation, namely the *allegation*, the *counterevidence* and the *intermediate fine*. The allegation contains the alleged element and the motivation. A very similar structure is used by counterevidences, where only the allegation content is substituted by the evidence data. In this case, it may contain a testimony, a graphical proof (i.e. picture or video) or any probatory element. Regarding the intermediate fine, it is a revision of the initial fine based on the previous data elements. Thus, it is formed by the assessment of the counterevidences and allegations at stake and the revised fine amount.

In the Process resolution, apart from the aforementioned allegations, only the *final fine* is managed. The main difference between this structure and the previous one is that it establishes the definitive fine, showing its motivation. It also details the legal basis for the posterior appeals by the offender.

Finally, the Appealling phase manages the *appeal* and its *result*. Although the appeal has a different legal status, its contents are the same as the allegations one, except from the vehicle data. On the other hand, the appeal result mainly describes the appeal assessment by the Authority and the remaining legal actions that may be taken by the offender.

4.5 Enforcement entities

The entities that compose the enforcement system are organized in four blocks (see Figure 4.1), namely the Witness data retrieval, the Offender communication management, the Data management and the Enforcement process management. Following there is a description of each block.

4.5.1 Witness data retrieval

This block gathers the two entities (Evidence Collector and Data Requester) that communicate with the witness stakeholders (see lower left part of Figure 4.1). The Evidence Collector gathers the initial evidence, delivers it to the appropriate entity in the Enforcement process management group, and registers it within the Data management block.

The Data Requester retrieves additional information from stakeholders. It may be required by the Authority to contrast a given allegation or counterevidence. It may also enable the offence-related stakeholders to contact with witnesses to retrieve information for a later counterevidence.

4.5.2 Offender communication management

The two entities (Notifier and Designated-as-offender contact point) that enable the communication with the offence-related stakeholders are placed here (see lower right part of Figure 4.1). The Notifier performs the legal notification of every fine (initial, intermediate, final) and resolution (appeal resolution). The Designated-as-offender contact point allows the offence-related stakeholders to introduce allegations, counterevidences and appeals.

4.5.3 Data management

This block is formed by three entities that manage all the process-related data (see right part of Figure 4.1). First, the Designated-as-offender personal data manager gathers all the personal data (including the driving licence information) related to the designated-as-offender. Second, the vehicle data is managed in the Vehicle data manager. These two entities may be implemented using national registers or the EUCARIS database. Third, the Process data manager stores the data exchanged with stakeholders, and the results of such transmissions, thus ensuring the process traceability.

It should be noted that the Designated-as-offender personal data manager is closely related to another entity which is in charge of managing the credentials associated with persons. Analogously, the Vehicle data manager cooperates with the entity that manages the vehicular credentials. Such entities are not depicted in

Figure 4.1 as they are not exclusive of the enforcement context, but instead shared with all the remaining management processes of the Traffic Authority.

4.5.4 Enforcement process management

This block is divided into four groups, each one called as the phase which it is related to (see upper part of Figure 4.1). The Starting group contains two entities. First, the Evidence analyser completes the offender personal data and vehicle description (if not contained within the initial evidence) and scrutinizes the evidence authenticity and its reliability. In case that this evidence is determined to be valid, the Initial fine issuer establishes the initial fine considering the described facts and the legislation in force.

The Preliminary investigation group is formed by four entities - the Liable driver analyser, the Counterevidence analyser, the Allegation analyser and the Intermediate fine issuer. The Liable driver analyser receives allegations that identify another person as the offending driver. This entity verifies the plausibility of such identification trying to decrease the chance of frauds. The remaining allegations are evaluated by the Allegation analyser, which establishes their authenticity and their relevance in the process. The Counterevidence analyser operates in the same way over the counterevidences. Based on their evaluation results, the Intermediate fine issuer confirms, revokes or decreases the initial fine.

The Process resolution contains the Process analyser and the Final fine issuer. The former revises the process development and determines if the legal framework has been respected. Excessive delays or unreliable data elements are examples of illegal process executions. Moreover, it evaluates the allegations sent after the Intermediate fine. Using these analysis results, the Final fine issuer establishes the final fine. Although the task performed by this entity is quite similar to that of the Intermediate fine issuer, they must be independent entities to mitigate the threat of collusion.

Finally, in the Appealling group the Appeal analyser determines the relevance of a given appeal and, based on such assessment, the Appeal result issuer definitively confirms or cancels the fine.

4.6 Data security and privacy analysis

Data security and privacy are paramount in the enforcement process. First, because of the legal consequences it may have. Second, because during the process, entities must deal with personal data of the designated-as-offender, the human witnesses, etc. The detailed model just presented allows to perform a preliminary analysis of these issues, which is presented in this subsection. First, the specific security and privacy goals that should be fulfilled are introduced. Afterwards, the threats that put at risk these goals are described, along with the corresponding countermeasures.

4.6.1 Goals

Apart from the reliable offender identification, there are four goals that must be achieved within the process development. First, the *privacy protection* (i.e. the right of an individual to control who has access to his or her personal information and under what circumstances [50]) must be fulfilled for all involved physical persons (i.e. the offender and the human witness, if any). This requirement has already been set for all applications of the aforementioned ITS technologies [2]. A related (but different) goal is the need of *confidentiality*, which implies that only the entities involved in the creation or delivery of a data element (according to the data exchanges defined in Appendix C) may be able to access it. The legislation regarding personal data protection does not impose the need for encryption to provide confidentiality over data which is related to an administrative punishment[1] [52]. However, it seems a reasonable practice to require the more strict security goals whenever they do not imply an excessive, unjustified overload on the implementing

[1] For an in-depth explanation on the security implications of the aforementioned legislation, please refer to [51].

systems. For this reason, providing confidentiality is set as the second goal in this model.

The third goal is that all the data at stake must be *trustworthy*, which implies that the information is created by an authorized sender and that the content is reliable. In particular, all the fines and the appeal resolution should be properly issued by the corresponding Authority and it should exist a method to verify their content. On the other hand, all the data inserted by witnesses and the designated-as-offender must faithfully describe the offence, its context and identify the offender. Otherwise, the whole enforcement process would be unreliable, thus losing its effectiveness.

The last goal refers to the *non-repudiation*, that is, avoiding an entity to deny having performed some action [53]. In particular, all the data exchanges between entities and stakeholders must be non repudiable regarding origin (i.e. avoiding the false denial of having created and sent a message) and receipt (i.e. avoiding the false denial of having received a message). In this way, the possibility of denying the relationship with some data exchange is prevented. Particularly, this goal ensures a complete traceability of the data exchange process, as both the sending and receiving operations may be accurately traced back to their originating parties. Such traceability is critical in a potential dispute resolution process related to this issue. For example, the offender may claim not having received the notification to allege that the process is not conforming to the legislation and thus it should be invalidated.

4.6.2 Threats and countermeasures

Each of the aforementioned goals has some threats that make its achievement harder. Such threats are described below, along with countermeasures that may be applied to mitigate them.

Regarding the personal privacy, the threat of *tracking* (i.e. to discover the path that has been followed by a given vehicle) has raised a remarkable concern among researchers [54]. Regarding the offender, it may happen if not privacy-respectful surveillance methods are employed to detect offences. Although this threat may always exist in the physical environment (as it may be possible to install a network of surveillance cameras), the use of pseudonyms has been proposed to mitigate it in the electronic vehicular network [54].

With respect to the data confidentiality, the *unauthorized data disclosure* threat allows undesired third parties to access to confidential information. Although each entity participating on a data exchange is subject to this threat, in this context it is specially focused on the Data Management entities (see Section 4.5), as they hold all the data related to the process, the existing drivers and their vehicles. Thus, protection mechanisms such as access control measures must be put in place to mitigate this threat. Moreover, such confidentiality may also be provided during all the associated data exchanges. Depending on the underlying reliability of the communication network, this threat may be present to a different extent. In any case, encryption techniques may be applied to mitigate this threat.

The *false data spreading* is a threat against the data trustworthiness that can be employed by any stakeholder to alter the regular process development. In this context, this threat may be interesting for the offender, as she may try to avoid the fine by sending a false (beneficial) counterevidence in case that the illegal action was really done. It may also be employed by a human witness to falsely accuse a person of having committed an offence. In order to mitigate this threat, the use of plausibility checks has been proposed to assess the reliability of a given sensorial data, such as those that may be employed in this context [17].

Finally, the *repudiation* threat may be present in the behaviour of the offender, the witness and the Authority in general. Regarding the offender, she may claim that she did not receive any notification, as a means of invalidating the whole process. With respect to the witness, it may deny having created a testimony once it is found to be false. Related to the Authority, it may deny having received a counterevidence as a way of imposing the maximum punishment and thus maximizing the economic revenue. In order to avoid this threat, non-repudiation mechanisms must be introduced in the data exchanges of the enforcement process [55].

4.7 ITS-based enhancements on enforcement systems: Integration in the proposed model

This Section focuses on how ITS-related technologies may contribute on solving the problems of current enforcement systems described in Section 3.4. Moreover, the parts of the model affected by each of these improvements are identified.

4.7.1 Improvements on offender identification

ITS-related identification techniques for vehicles (EVI) and also for its driver (electronic identification card or electronic driving license), enable a more immediate electronic offender identification. An automatic remote verification may be performed using the Driver credentials reader, as envisioned by TISPOL[2]. Such identification is required for offences related to the traffic rules, where the driver is the responsible person. In this way, notifications could be referred to the actual driver, avoiding the need for the vehicle holder to nominate her afterwards. However, it raises privacy concerns as it would enable tracking a given person. The development of a privacy-compliant enforcement process is a matter of open research. Particularly, the PRECIOUS research project funded by the Autonomous Community of Madrid is focused on using anonymous credentials to enable a privacy-respectful remote verification of vehicular authorizations [56].

[2] https://cleopatra.tispol.org/cleopatra/europe/general/technology/identifying-and-fining-owner-vehicle/identifying-and-fining-owne, accessed on January 2012

Integration in the proposed model

Apart from the Offending vehicle (which should be ITS-enabled, as described in Section 2.2.4), only the Automatic sensor devices are affected as they should perform the electronic authentication protocol. The remaining entities (starting by the Evidence Collector) are not aware of this issue as the *initial evidence* structure was already prepared to contain the real offender identification.

4.7.2 Improvements on notification delays

ITS communication technologies are suitable to timely send notifications to the offender through her vehicle. Even if the speed of this transmission is subject to the availability of network and computational resources, the message may be delivered either during the journey or, if required, using periodic resilient connections (i.e. gas or electricity stations). Moreover, the vehicular human-machine interface may present notifications in real time without causing a distraction.

Integration in the proposed model

The notification improvements only affect to the Offending vehicle (which should be again ITS-enabled, as described in Section 2.2.4) and the Notifier. The first one should be ready to receive (and present to the driver) the notification message. The Notifier encapsulates the mechanism to deliver such message to the appropriate stakeholder. Thus, any future variation on this mechanism would be confined in this entity.

4.7.3 Improvements on the offence description and the lack of witnesses

In-vehicle sensors and the data shared through VANETs may help on the offence description. Thus, sensors may give a complementary description of the situation from inside the vehicle [17]. Even if sensorial errors may happen, several surrounding vehicles may be contacted to gather their viewpoints, thus clarifying the situation.

Integration in the proposed model

The use of vehicular sensorial data may be implemented through the interaction between the Surrounding vehicles (which will offer the information using the ITS equipment) and the Data Requester (which will gather it).

4.8 General model for the remaining contributions of this thesis

Contributions C2, C3 and C4 (recall Section 1.3) of this thesis are focused on different protocols and mechanisms that address the implementation of parts of the road traffic enforcement process. In this Section, the parts of the model related to each contribution are identified (Section 4.8.1). On the other hand, from the vehicular point of view there are several decisions and assumptions that have to be taken. They conform the technical framework in which the proposed contributions will be applied. Section 4.8.2 introduces a summary of these decisions and assumptions. However, in order to ensure that each Chapter describing the remaining contributions is self-contained, the particular model and considerations that affect to each of them will be detailed in each Chapter.

4.8.1 Parts of the enforcement model related to each of the proposed mechanisms

Figure 4.2 depicts graphically the parts of the model related to each contribution. First, the steganographic mechanism that enables the covert reporting of misbehaving vehicles is a way to enable witnesses to send evidences that may indicate that an offence has been committed. Thus, the parts of the model related to this contribution are, apart from the ITS-enabled vehicle (which will act as the offence witness), the Evidence Collector (EC) and the Evidence Analyser (EA). It should be noted that the complete analysis that should be conducted (by the EA) to determine the reliability of the data at stake is out of the scope of this thesis. However, as the extraction of the embedded data (that is, recovering the evidence data itself) is also addressed by this contribution, we find that such process could be a collaborative task between EC and EA – although it is a prerequisite for the analysis itself, this task is conceptually bigger than the responsibility assigned to the EC.

Concerning the notification protocol, the enforcement entities related to this contribution are the respective message issuers (especially the Initial Fine Issuer, although it may be adapted to serve for the Intermediate Fine Issuer, the Final Fine Issuer and the Appeal Result Issuer), the Notifier, the ITS-enabled vehicle and its driver. Specifically, the fine issuers act as the message generator, whereas the Notifier delivers it. The vehicle will receive the notification and will transmit it (in a way compatible with the task of driving) to the driver.

Finally, the cooperative evidence generation protocol affects to the ITS-enabled vehicles, the Data Requester, the Designated-as-offender Contact Point (DCP) and the CounterEvidence Analyser (CEA). Thus, ITS-enabled vehicles will get in contact and will send their corresponding data to the CEA through the Data Requester (for the witness stakeholders) and the DCP (for the offence-related stakeholder). The CEA will be in charge of verifying these data, as a preliminary step for the future adjudication process made by the Intermediate Fine Issuer.

4.8.2 Decisions and assumptions on the vehicular environment

Concerning the vehicular environment, there are several issues that have to be defined in order to determine the real scenario in which the remaining contributions may be applied. They affect to the reliability of the vehicular components, the management process for the vehicular credentials and the organization of the vehicular infrastructure.

In general terms, the set of vehicular devices are organized following the OVER-

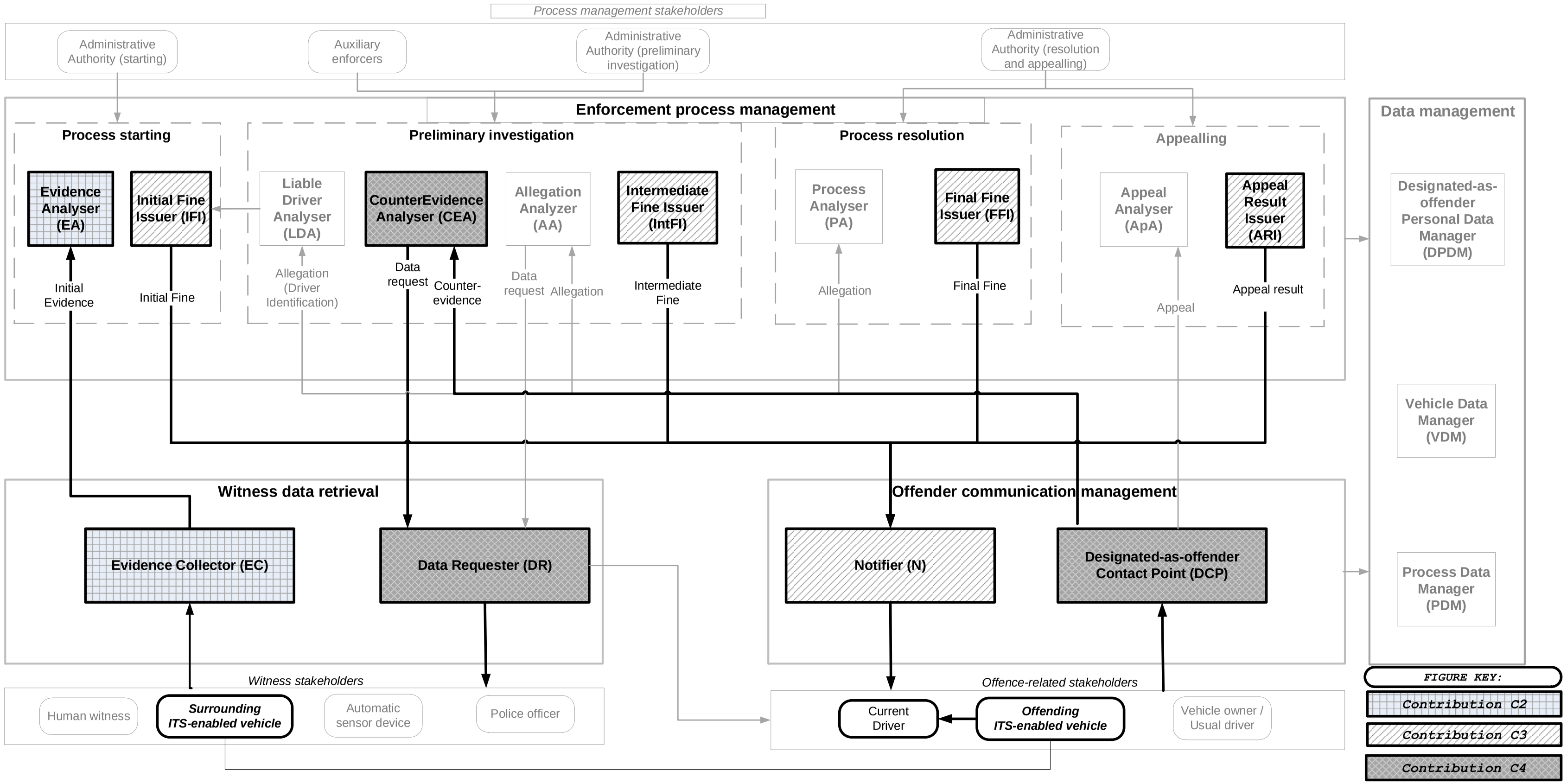

Process management stakeholders
Administrative Authority (starting)
Auxiliary enforcers
Administrative Authority (preliminary investigation)
Administrative Authority (resolution and appealling)
Enforcement process management
Process starting
Evidence Analyser (EA)
Initial Fine Issuer (IFI)
Initial Evidence
Initial Fine
Preliminary investigation
Liable Driver Analyser (LDA)
CounterEvidence Analyser (CEA)
Allegation Analyzer (AA)
Intermediate Fine Issuer (IntFI)
Allegation (Driver Identification)
Data request
Counter-evidence
Data request
Allegation
Intermediate Fine
Process resolution
Process Analyser (PA)
Final Fine Issuer (FFI)
Allegation
Final Fine
Appealling
Appeal Analyser (ApA)
Appeal Result Issuer (ARI)
Appeal
Appeal result
Data management
Designated-as-offender Personal Data Manager (DPDM)
Vehicle Data Manager (VDM)
Process Data Manager (PDM)
Witness data retrieval
Evidence Collector (EC)
Data Requester (DR)
Offender communication management
Notifier (N)
Designated-as-offender Contact Point (DCP)
Witness stakeholders
Human witness
Surrounding ITS-enabled vehicle
Automatic sensor device
Police officer
Offence-related stakeholders
Current Driver
Offending ITS-enabled vehicle
Vehicle owner / Usual driver
FIGURE KEY:
Contribution C2
Contribution C3
Contribution C4

Figure 4.2: Parts of the model produced in contribution C1 related to contributions C2, C3 and C4.

SEE architecture (recall Section 2.2.4). It should be noted that it does not only determine the way in which these devices are organized, but also their assumed degree of reliability. Particularly, the Hardware Security Module (HSM) is assumed to be protected against manipulation. The HSM also provides with a secure storage which is used to store vehicular credentials. Concerning these credentials, it is assumed that vehicles will be identified by means of a set of short-lived pseudonyms. They have an associated public-private keypair, which is certified by means of a public key certificate. Such credential is issued by the traffic authority, and it is assumed that a preloading operation is performed in such a way that they are securely transferred to the HSM prior to their use in the contributions presented herein.

Related to the vehicular infrastructure, it is assumed that there will be a set of RSUs available to participate in the proposed protocols and mechanisms. Such RSUs are assumed to be independent one to each other. In other words, there is no interconnection among these devices.

On the other hand, it is assumed that there exists a reliable entity in the infrastructure, which is trusted to take a fair decision whenever several (potentially contradictory) descriptions of one situation are given. Particularly, it will be present in both the notification and the evidence generation mechanisms. In general words, it will be accessible by vehicles through a resilient communication channel, that is, a channel that ensures that the data is delivered after a finite amount of time. Thanks to this assumption, it is possible to establish the cause of an unsuccessful data exchange that is performed over an unreliable network (such as the vehicular, DSRC-based one). Such failure may be caused by the unreliability of the network or because the vehicular device was not working properly. It should be noted that in the second case, some consequences may be applied over the vehicle, starting by calling it for maintenance in order to reset the vehicular communication devices.

In order to ensure that the aforementioned reliable channel exists, it is assumed that vehicles will get connected to this channel periodically, typically at a daily basis (e.g. at the end of the day, using the wireless connection of the parking lot).

4.9 Summary of the chapter

In this Chapter, an enhanced enforcement model has been proposed based on the previous VERA2 one. Such model is composed by a set of refinements over the VERA2 model (to make it suitable to current Spanish legislation), the stakeholders, the enforcement entities, the data at stake including their interchanges and their security and privacy concerns. Based on this model, it has been discussed the way in which ITS technologies may help on addressing the problems of the enforcement process, and how they would be integrated into the proposed model. Furthermore, as the presented model is the basis for the remaining contributions of this thesis, the parts of such model that are at stake on each contribution are identified. The set of general assumptions that are considered in such contributions is also identified.

Chapter 5

Mechanism for covert reporting of misbehaving vehicles

Despite the huge promise of ITSs, some road safety related applications cannot be currently developed in VANETs. One example of these applications is the automatic reporting of misbehaving drivers by other drivers (or their vehicles). The reasons are illustrated next: Consider a dangerous driver that is not respecting some essential rules like the safety distance or that performs unsafe overtaking. It would be quite interesting for observing drivers to report this attitude, as it is done in [57]. In this way, police patrols could be more effective in their surveillance tasks, removing such undesirable attitudes from the road more efficiently.

Although this application is beneficial for road safety, drivers would rarely send these report messages over a VANET. This is because the reporting message can be observed by the dangerous driver himself. Thus, he can decide to take reprisals against the reporting vehicle. Even if encryption is applied, the mere detection of an encrypted message can raise suspicions on the reported vehicle. It would therefore be useful to introduce a mechanism that allows VANET users to send messages through the VANET while remaining hidden for those that are not the expected receivers.

Steganography is a technique that allows hiding data within an innocuous message called *cover*. Thus, hidden data remain undetectable for unauthorized parties. To the best of the author of this thesis' knowledge, the use of steganography in this specific kind of network has not been explored yet.

The use of systematic encryption (that is, sending an encrypted reporting message at a fixed time interval [58]) could be an alternative to such steganography-based approach. However, the efficiency of such a system could be low if the amount of reports is small compared to the aforementioned time interval. In such situation, most messages would not contain meaningful information but they should be sent anyway. As the occurrence of reportable actions is not periodic, there will always periods in which it would not be necessary to send any encrypted message. For this reason, such solution is undesirable for a vehicular scenario, in which saving bandwidth and computation is critical to ensure the proper operation of safety-related ITS applications.

Taking into account the previous considerations, in this Chapter a steganography-based mechanism for covert reporting of misbehaving vehicles is presented. The mechanism enables the transmission of the main data that describe the offence (i.e. perceived offence and the alleged offender identifier). Other supporting data (such as pictures) must be sent using an alternative channel. The scope of this mechanism is the embedding and revealing operations. Therefore, the posterior processing of the embedded report and particularly its trustworthiness analysis is left to future work. Section 5.1 gives an overview of the proposed inter-vehicle reporting application. Section 5.2 identifies the parts of the entities model proposed in Chapter 4 that are related to this mechanism, as well as the considered architecture. The following sections focus on the mechanism itself, describing respectively the secret message M structure (Section 5.3), the cover message C and its capacity (Section 5.4), how the secret message is protected (Section 5.5), and, finally, the embedding and revealing functions F_e and F_r (Sections 5.6 and 5.7).

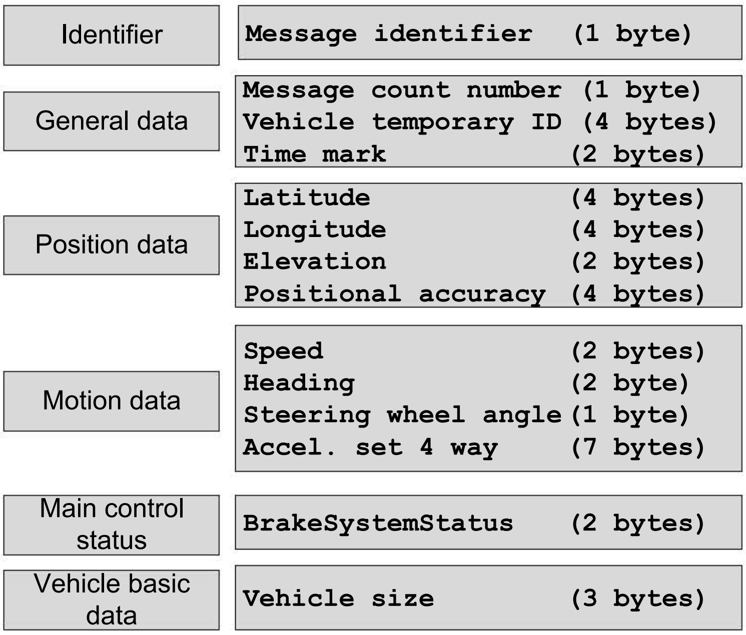
5.1 System overview

The proposed system enables a vehicle to covertly send a report of another misbehaving vehicle to a Road-Side Unit (RSU). For this purpose, a source of redundancy is required to embed information without altering the intended purpose of the cover data. In the VANET domain, measurements from in-vehicle sensors are prone to inaccuracies. These measurements could be changed without altering significantly the reliability of the data at stake. Particularly, in the proposed system, to minimize the consequences of the embedding operation, the least significant bits of sensorial data fields are altered such that the distance of the new provided value to the original one is within the accuracy of the sensorial measurement. Such decision limits the capacity of each data field to embed secret data. For this reason, this mechanism is intended to enable vehicles to send the minimum set of data that describes the offence (e.g. the misbehaving action and the purported offender identifier). Other supporting data, such as pictures, should be sent using an alternative channel, such as a cellular one. Such channel must ensure that the offender is unable to detect the transferred message and must offer an acknowledged reception, which enables the reporting vehicle to delete the data at stake.

The VANET message which has more sensorial information is the *beacon*. Essentially, a beacon contains the current speed, location and heading of the sender vehicle. The sensorial data is obtained first by the Event Data Recorder (subject to IEEE 1616 [22]) and then the beacon message is constructed according to the SAE J2735 standard [59]. Figure 5.1 shows the beacon structure without optional parts.

Beacons are received by any other VANET entity (i.e. OBU or RSU) which is located within a range of 1 kilometre [59]. As they are sent at a high frequency (one each 100 ms), they enable an almost constant channel with surrounding parties. Particularly, reporting messages will be prepared to be sent to nearby RSUs. As RSUs are usually assumed to be reliably connected to the Authority, this allows distributing the workload among them at the same time that it is assured that the Authority will receive the reports.

To protect the secret message from unauthorized access, it will be encrypted



Identifier	Message identifier	(1 byte)
General data	Message count number Vehicle temporary ID Time mark	(1 byte) (4 bytes) (2 bytes)
Position data	Latitude Longitude Elevation Positional accuracy	(4 bytes) (4 bytes) (2 bytes) (4 bytes)
Motion data	Speed Heading Steering wheel angle Accel. set 4 way	(2 bytes) (2 byte) (1 byte) (7 bytes)
Main control status	BrakeSystemStatus	(2 bytes)
Vehicle basic data	Vehicle size	(3 bytes)

Figure 5.1: Beacon structure without optional parts

using ECIES (Elliptic Curve Integrated Encryption Scheme). The main reason for this choice is that it is the only encryption technique among those proposed in the IEEE 1609.2 VANET security standard that allows an unnoticed online key agreement, thus avoiding the need to count with a preshared secret [8]. Additionally, as all VANET participants should comply with this standard, the selection of ECIES guarantees that they will be able to execute the required cryptographic operations.

Replacing the least significant bits of sensor measurements introduces errors that can affect road safety. To minimize this effect, a maximum rate of messages (embedding interval K) that may contain embedded information can be imposed[1]. Moreover, as VANET communications suffer from certain degree of unreliability, it is necessary to introduce a mechanism that guarantees with some probability that a report message is received by the RSU. For the sake of simplicity, in the proposed system each report message is sent R times. Other alternatives to contribute on

[1] Note that reducing the number of least significant bits used to embed information would also reduce the introduced error.

ensuring the reception of this message are studied in Section 5.6.

In order to guarantee that the embedded message is not detected, no statistical differences should exist between the original cover data and the embedded data. In this work it is assumed that the inaccuracies (or errors) present in the sensor measurements are random. Therefore, as the message to be embedded is composed by encrypted data and a message authentication code, it is also random by nature and no statistical differences should exist in theory. However, in the cases that this assumption is not hold, techniques as the ones described in [60] could be applied.

5.2 Model and architecture

In this Section, the considered model and architecture are presented. The entities at stake, along with their architectural realization, are presented in Section 5.2.1. Afterwards, the requirements that have to be fulfilled are described in Section 5.2.2. Finally, the working assumptions are introduced in Section 5.2.3.

5.2.1 Participant entities

The parts of the entities model of the enforcement process that are related to this mechanism are highlighted in Figure 5.2. Thus, an ITS-enhanced surrounding vehicle, which has been victim of an offence, is able to send to the Evidence Collector (EC) the corresponding embedded report. This entity will be in charge of, first, extracting such information from the cover message and, second, of delivering these data to the Evidence Analyzer (EA). The latter will evaluate the received report.

The proposed mechanism is focused on the communication between the vehicle and the RSU, which will act as the receiver of the embedded report (i.e. EC). The communication between EC and EA (i.e. the processing systems of the Traffic Authority) will not be considered. Therefore, the architecture is formed by two elements, namely the vehicle and the RSU, which are communicating through a VANET using DSRC as the underlying transmission technology. Concerning the

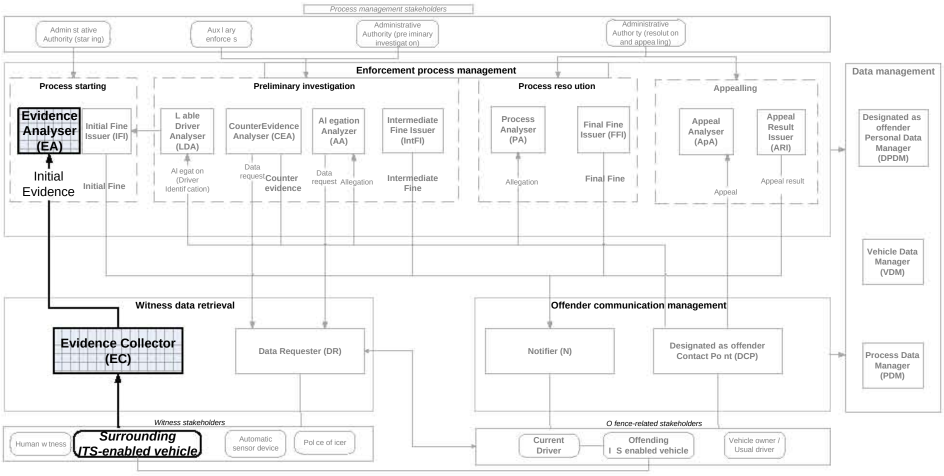

Process management stakeholders
Admin st ative Authority (star ing)
Aux l ary enforce s
Administrative Authority (pre iminary investigat on)
Administrative Author ty (resolut on and appea ling)
Enforcement process management
Process starting
Evidence Analyser (EA)
Initial Fine Issuer (IFI)
Initial Evidence
Initial Fine
Preliminary investigation
L able Driver Analyser (LDA)
CounterEvidence Analyser (CEA)
Al egation Analyzer (AA)
Intermediate Fine Issuer (IntFI)
Al egat on (Driver Identif cation)
Data request
Counter evidence
Data request
Allegation
Intermediate Fine
Process reso ution
Process Analyser (PA)
Final Fine Issuer (FFI)
Allegation
Final Fine
Appealling
Appeal Analyser (ApA)
Appeal Result Issuer (ARI)
Appeal
Appeal result
Data management
Designated as offender Personal Data Manager (DPDM)
Vehicle Data Manager (VDM)
Process Data Manager (PDM)
Witness data retrieval
Evidence Collector (EC)
Data Requester (DR)
Offender communication management
Notifier (N)
Designated as offender Contact Po nt (DCP)
Witness stakeholders
Human w tness
Surrounding ITS-enabled vehicle
Automatic sensor device
Pol ce of icer
O fence-related stakeholders
Current Driver
Offending I S enabled vehicle
Vehicle owner / Usual driver

Figure 5.2: Parts of the entities model of the enforcement process related to the proposed reporting mechanism

vehicle, it follows the OVERSEE architecture as described in Section 2.2.4. Particularly, apart from the in-vehicle sensors, three elements will be involved in this architecture, namely the Secure Application Environment (SAE), the Hardware Security Module (HSM) and the On-Board Unit (OBU). Particularly, the SAE holds the computer code that performs the embedding operation. The HSM performs the cryptographic operations and the OBU serves as the communication unit to transmit data to other entities, particularly the RSU for the context of this contribution.

5.2.2 Requirements

Based on the desirable properties of any steganographic system (Section 2.3.3) and the purpose of the considered application, a set of requirements to be fulfilled is established:

Undetectability. The reporting message must remain undetectable to the reported vehicle.

Maximum capacity. The proposed mechanism must provide with the maximum capacity. This requirement must not threat the undetectability one.

Computational feasibility. The embedding operation must be computationally feasible for the sender. Similarly, the revealing procedure must be feasible for the receiver.

Resistance against data losses. The proposed mechanism must counter (as much as possible) the data losses that may happen in transmissions over unreliable channels.

Embedded message integrity. The proposed mechanism must be able to detect any manipulation over the embedded report.

5.2.3 Working assumptions

The proposed mechanism is to be executed where the following two assumptions hold. First, it is assumed that RSUs are able to interact with the certification authority to determine whether two pseudonyms belong to the same entity. Second, even if the receiving entities may be different RSUs, it is assumed that if a message is sent to a specific RSU it is not received by any other one. It avoids unnecessary burden on RSUs, which could compromise the feasibility of this mechanism.

5.3 Secret message structure

The misbehavior report to be embedded contains the following fields:

- *Magic header* (16 bits), which helps the receiver on identifying whether there is an embedded message or not. The probability of finding a beacon that does not include the beginning of a reporting message but includes the aforementioned magic header is 2^{-16}.

- *Message type* (4 bits), as there may be other applications enabled by this steganographic scheme, a message type field has been introduced.

- *Misbehaving action* (4 bits), it will identify the type of misbehaving action that it is reported.

- *Message payload* (32 bits), in this case it will be filled with the misbehaving vehicle identifier. Although this is a pseudonym and may change over time, it is the only identifying information from the misbehaving vehicle available to the reporting one.

5.4 Cover message and capacity analysis

In the proposed system, beacon messages are selected as covers because they contain sensorial data (positioning, speed, heading...) subject to inaccuracies (or errors). In order to covertly send information, in this work it is assumed to be acceptable to change the value provided by the sensors $v_{measured}$ to a value v_{stego} that is within the range determined by the sensor's accuracy *accy*, i.e., $v_{stego} \in [v_{measured} - accy, v_{measured} + accy]$.

The capacity of one data element d_i (see Equation 5.1), i.e., the number of values that can be encoded in certain sensorial data element, will be given by the ratio between the accuracy *accy* of the element and its resolution *res* plus one (to take into account the value provided by the sensor).

$$Capacity_{d_i}(bits) = \lfloor log_2 \left(\frac{accy_{d_i}}{res_{d_i}} + 1 \right) \rfloor \qquad (5.1)$$

It must be recalled that the sensorial data is obtained first by the Event Data Recorder (subject to IEEE 1616 [22]) and then the beacon message is constructed according to the SAE J2735 standard [59]. To calculate the capacity of each sensorial data element we have analysed the accuracy and resolution defined in the aforementioned standards. While the EDR standard establishes the required resolution and accuracy, the J2735 standard describes only the resolution of each field. Thus, in the calculations, the accuracy described in the IEEE 1616 standard has been used. We assume that vehicles' sensors are compliant with these standards. Table 5.1 specifies the maximum capacity of each beacon sensor field and the whole capacity of the message, 24 bits, considering the minimum capacity provided by both standards (as it is not assumed a specific point in the process to insert the covert information and it must be preserved in all cases).

Considered sensorial fields	**Ratio** $\frac{accy_{IEEE1616}}{res_{IEEE1616}}$	**Ratio** $\frac{accy_{IEEE1616}}{res_{J2735}}$	**Capacity IEEE 1616**	**Capacity J2735**	**Maximum introduced error**
Latitude	600	600	**9 bits**	9 bits	0.0512' = 94.8 m
Longitude	600	600	**9 bits**	9 bits	0.0512' = 94.8 m
Speed	50	180	**5 bits**	7 bits	0.64 m/s = 2.34 km/h
Heading	10	91	3 bits	**0 bits**	–
X Acceleration	0	9	**0 bits**	3 bits	–
Y Acceleration	0	9	**0 bits**	3 bits	–
V Acceleration	0	1	**0 bits**	0 bits	–
Yaw Rate	1	10	**1 bits**	3 bits	0.1 °
Overall (independ.)			**27 bits**	**34 bits**	
Overall (combined)			**24 bits**		

Table 5.1: Capacity of each beacon sensorial data field calculated according to Eq. 5.1 and overall capacity of beacon messages. The maximum error that could be introduced in the proposed steganographic system is also presented (it is equal to $accy_{IEEE1616}$).

5.5 Protecting the secret message

In this work, ECIES is used to protect the secret message before embedding it. ECIES uses public key cryptography to derive two keys that will be used for symmetric encryption and message authentication. As it is based on elliptic curves, it usually requires a lower computational effort compared to other traditional encryption schemes. Several data are used as input of the key derivation process. Besides the ECIES public parameters (which should be previously known by all parties), the sender vehicle requires to have its private key, the public key of the receiver RSU, and a salt value. On the other hand, the receiver RSU requires to have the public key of the sending vehicle, its private key and the salt value. In order to guarantee that these data is available to the interested parties, several decisions and assumptions have been taken, as explained next.

In the proposed system, it is assumed that the public key of the RSU is made available to vehicles by means of the periodical WAVE Service Announcements sent by the RSUs [61]. On the other hand, we assume that each beacon is signed by the vehicle (to avoid the threat of data forgery, as explained in IEEE 1609.2) and that the signature includes the vehicle's public key certificate. Regarding the salt, the beacon ID (B_{ID}) of the first beacon used to embed the secret message has been selected.

Once the secret key has been derived, the reporting message is symmetrically encrypted. As ECIES enables using a stream cipher combined with the aforementioned key derivation function, the XOR (or-exclusive) operation has been selected. The resulting encrypted message has the same bit length than the secret message, that is, 56 bits. Additionally, as established by ECIES standard, a message authentication code of 160 bits[2] is appended to the encrypted message. Therefore, the final message to be embedded within the cover has a total length of 216 bits (see Figure 5.3).

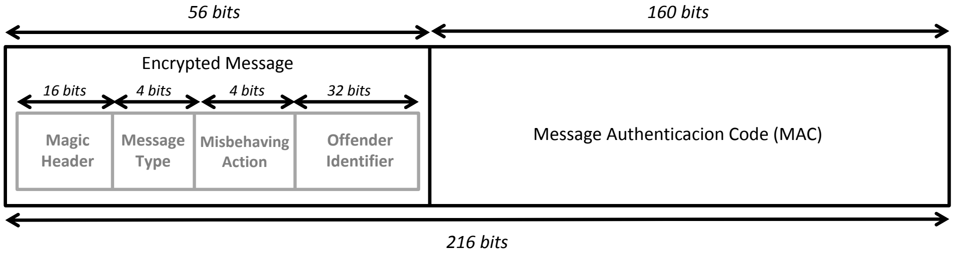


Figure 5.3: Structure of the reporting message to embed into beacon messages

As the length of the protected message exceeds the capacity of a beacon message, more than one beacon is needed to embed it. The total amount of required beacons is $nb_{msg} = 216\ bits/msg \div 24\ bits/beacon = 9\ beacons/msg$.

It should be noted that the reduced length of the reporting message makes that

[2] 160 bits is the output length of the MAC1 function that may be selected for ECIES according to the IEEE 1363 [62].

even if the witnessed offence is repeated over time, it would not be more efficient to send an *offence reconfirmation* message (i.e. expressing “I have witnessed again the same offence that I have already reported”) instead of repeating the whole reporting message again.

5.6 Embedding function

In this Section, the operation concerning the insertion of secret data within the cover message is described. One of the key aspects of the proposed mechanism is that it must counter (as much as possible) the channel unreliability. Section 5.6.1 analyses the alternatives to promote the message reception, whereas Section 5.6.2 describes the internals of the whole embedding procedure.

5.6.1 Alternatives to promote the message reception

In order to ensure that the message is received over an unreliable channel, several alternative mechanisms may be used. All of them are based on the assumption that the more times a message is sent, the higher the probability of reception is.

The simplest decision is to repeat the message a given amount of times ([63], Chapter 1). In the analysed application, it means that the whole set of fragments should be repeated one or more times. The simple message repetition scheme has a low efficiency, in that it requires to linearly multiply the amount of network resources as much as the amount of repetitions.

In order to promote a correct reception of a message through a noisy channel while providing a reasonable efficiency, there is a set of correction codes that may be applied. In this field, Low-Density Parity Check (LDPC) ([63], Chapter 47) and repeat-accumulate codes ([63], Chapter 49) have been intensively studied. In a nutshell, these techniques enable recovering some parts of the received message because several dependences are established between the values of different parts. In this way, if one part is not successfully received, it can be predicted by solving the corresponding dependences. It should be noted that if the value of the involved parts is not successfully received, a belief propagation process has to be executed. The efficiency of this kind of codes (especially LDPC) has turn them to be very useful for practical systems, such as digital television broadcasting.

Even if the efficiency of this kind of mechanisms outperforms the basic repetition scheme in terms of required network resources, for the sake of simplicity the latter will be selected in this thesis. Given that the ECIES algorithm is the public key encryption scheme selected in IEEE 1609.2 standard, and given that it provides not only confidentiality but also integrity (in that a Message Authentication Code is calculated, so transmission errors may be detected), introducing an additional computational workload could put the feasibility at risk. Nevertheless, the development of an efficient code correction technique suitable for this environment is left to future work.

5.6.2 Procedure

The embedding function protects first the secret message as described in Section 5.5. This operation is specified in Algorithm 1. Afterwards, the secret is split and the resulting fragments are embedded on nb_{msg} beacon messages. Embedding consists on replacing the least significant bits of the sensorial data elements with those of the protected secret message (see Algorithm 2). A graphical representation of the process is shown in Figure 5.4.

In order to minimize the introduced error, an embedding interval K has been defined. Bits of the protected secret message may only be embedded in beacons whose beacon ID B_{ID} is multiple of K.

Additionally, each secret message is sent R times to reduce the possibility of not receiving a reporting message due to communication errors. As the beacon ID B_{ID} of the first beacon in which the secret message is embedded is used as salt in the key derivation process, different keys are created for each message repetition.

It should be noted that the procedure described so far does not take into account whether a given repetition has been successfully received or not, before sending the following repetition. In other words, there is no acknowledgement mechanism which makes the sender aware of the reception and avoids further repetitions. Even if such mechanism would have a positive impact on the overall efficiency, it should be recalled that such acknowledgement must not be perceived by the reported vehicle. Given that RSUs do not issue beacons by themselves, the definition of a suitable RSU-originating cover message to convey this acknowledgment is left to future work.

```
Data: $PK_{Rcv}$, public key of the receiver; $PrivK_{Snd}$, private key of the sender;
      $M_1...M_{16}$, the magic header content; $B_{ID}$, beacon identifier; $R_1...R_{32}$,
      misbehaving vehicle identifier; $A_1...A_4$, perceived misbehaving action
begin
    Set MagicHeader ← $M_1...M_{16}$
    Set MessageType ← 0001
    Set MisbehAction ← $A_1...A_4$
    Set MessagePayload ← $R_1...R_{32}$
    # Secret keys derivation according to ECIES
    Set $SecretKey_1$ ← KDF1(Hash=SHA-256, $PrivK_{Snd}$, SVD($PK_{Rcv}$), $B_{ID}$)
    Set $SecretKey_2$ ← KDF2(Hash=SHA-256, $PrivK_{Snd}$, SVD($PK_{Rcv}$), $B_{ID}$)
    # Secret message encryption
    Set EncryptedMagicHeader ← MagicHeader ⊕ $SecretKey_2$ (bits 1...16)
    Set EncryptedMessageType ← MessageType ⊕ $SecretKey_2$ (bits 17...20)
    Set EncryptedMisbehAction ← MisbehAction ⊕ $SecretKey_2$ (bits 21...24)
    Set EncryptedMessagePayload ← MessagePayload ⊕ $SecretKey_2$ (bits
    25...57)
    Set EncryptedMessage ← EncryptedMagicHeader ‖
    EncryptedMessageType ‖ EncryptedMisbehAction ‖
    EncryptedMessagePayload
    # MAC1 calculation according to ECIES
    Set MessageAuthenticationCode ← HMAC(Hash=SHA-1, $SecretKey_1$,
    EncryptedMessage)
    Set MessageToEmbed ← EncryptedMessage ‖
    MessageAuthenticationCode
```

Algorithm 1: Secret message preparation algorithm

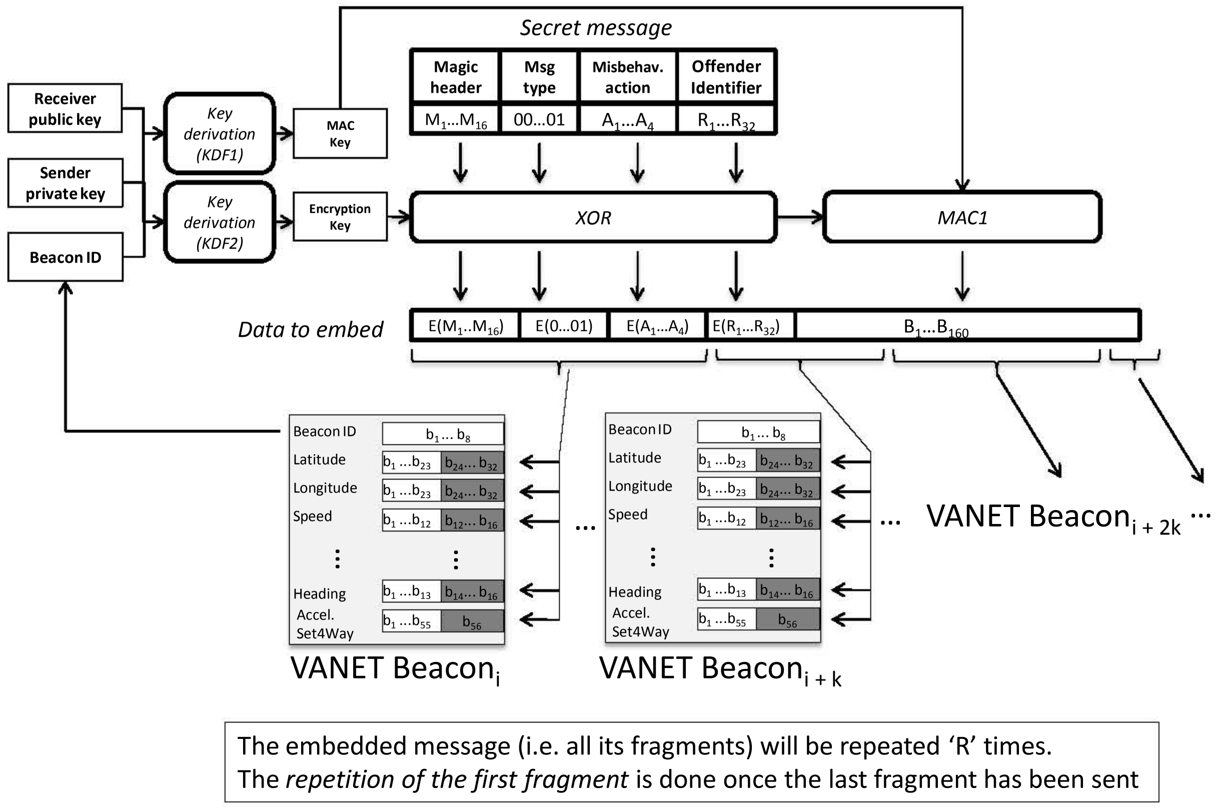


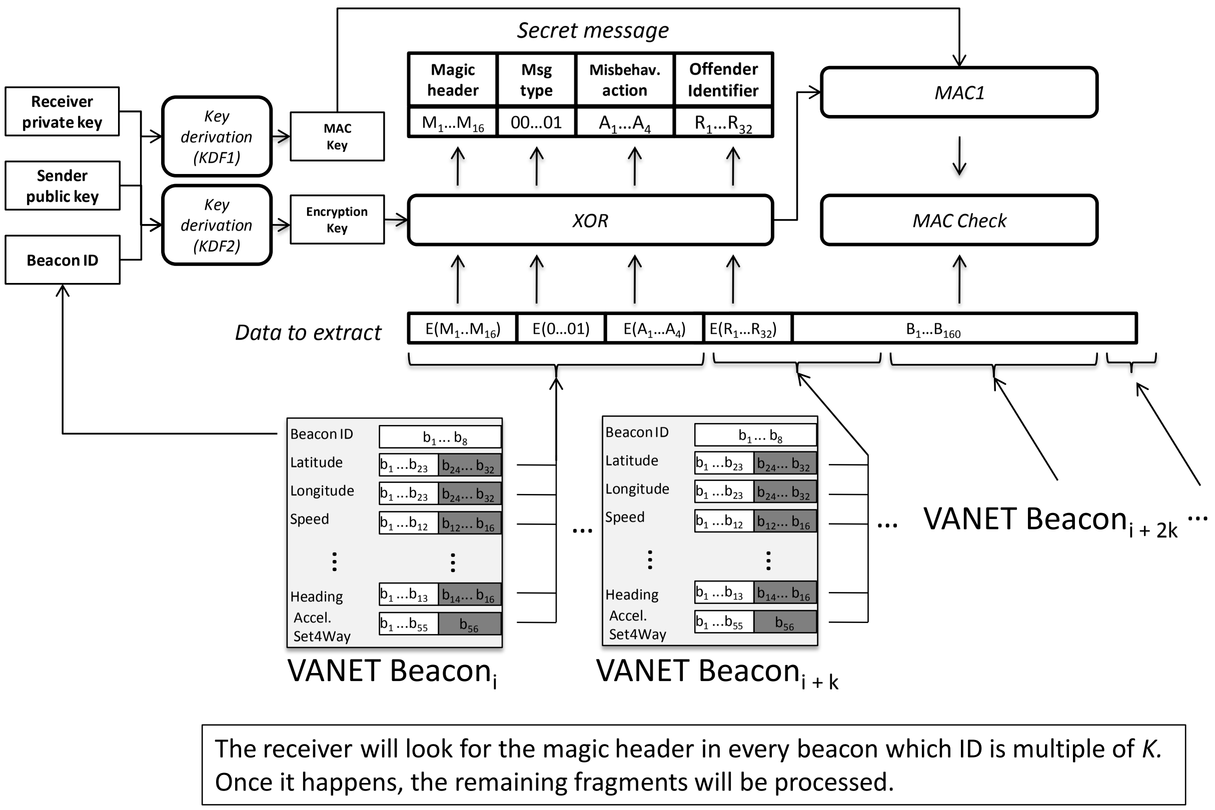
Figure 5.4: Embedding function including message fragmentation

```
Data: MessageToEmbed; MessageToEmbedLength, 216; K, embedding
      interval; $B_{ID}$, beacon identifier.
begin
    Set CurrentBit ← 0
    Set CurrentK ← 1
    Set BeaconToEmbed ← $B_{ID}$
    # The following operations will be repeated R times
    while CurrentBit less than MessageToEmbedLength do
        # After each embedding operation, it is checked (but omitted, for
        clarity) whether there are remaining bits to embed
        Set BeaconToEmbed.Latitude ← $B_{ID}$.Latitude (bits 1...23) ∥
        MessageToEmbed (bits CurrentBit...CurrentBit+9)
        Set CurrentBit ← CurrentBit+9
        Set BeaconToEmbed.Longitude ← $B_{ID}$.Longitude (bits 1...23)
        ∥MessageToEmbed (bits CurrentBit...CurrentBit+9)
        Set CurrentBit ← CurrentBit+9
        Set BeaconToEmbed.Speed ← $B_{ID}$.Speed (bits 1...11)
        ∥MessageToEmbed (bits CurrentBit...CurrentBit+5)
        Set CurrentBit ← CurrentBit+5
        Set $B_{ID}$.AccelSet4Way ← $B_{ID}$.AccelSet4Way (bits 1...55)
        ∥MessageToEmbed (bits CurrentBit...CurrentBit+1)
        Set CurrentBit ← CurrentBit+1
        if CurrentBit less than MessageToEmbedLength then
            Set BeaconToEmbed ← $B_{ID+CurrentK \cdot K}$
            CurrentK ← CurrentK + 1
```

Algorithm 2: Secret message splitting and embedding

5.7 Revealing function

The revealing function detects and decrypts embedded data within beacon, even in the case of fragmentation (see Figure 5.5 and Algorithms 3 and 4). The receiver does not know in advance if a reporting message is embedded in a cover. Thus, it must proceed as if any cover, among those eligible to contain embedded data (i.e. considering K), could contain the beginning of the secret. This is done by appending the extracted bits to a bitstream and by using a decryption window that moves along. If any of the beacons containing a message fragment is lost, the receiver will restart the whole revealing function.



The receiver will look for the magic header in every beacon which ID is multiple of *K*. Once it happens, the remaining fragments will be processed.

Figure 5.5: Revealing function including fragment reassembly

```
Data: PK$_{Rcv}$, public key of the receiver; PrivK$_{Rcv}$, private key of the
      receiver; PK$_{Snd}$, public key of the sender; B$_{ID}$, beacon identifier;
      M$_1$...M$_{16}$, the magic header content
begin
    Set EncryptedMagicHeader $\leftarrow$ B$_{ID}$.Latitude (bits 24...32) $\|$
    B$_{ID}$.Longitude (bits 24...30)
    # Secret keys derivation according to ECIES
    Set SecretKey$_1$ $\leftarrow$ KDF1(Hash=SHA-256, PK$_{Snd}$, SVD(PrivK$_{Rcv}$), B$_{ID}$)
    Set SecretKey$_2$ $\leftarrow$ KDF2(Hash=SHA-256, PK$_{Snd}$, SVD(PrivK$_{Rcv}$), B$_{ID}$)
    Set MagicHeader $\leftarrow$ EncryptedMagicHeader $\oplus$ SecretKey$_2$ (bits 1...16)
    if MagicHeader = $M_1$...$M_{16}$ then
        # Proceed to Embedded Message Extraction (Algorithm 4)
```

Algorithm 3: Embedded Message Detection Algorithm

```
Data: SecretKey$_1$, MAC key; SecretKey$_2$, decryption key; K, embedding
      interval; B$_{ID}$, beacon identifier; M$_1$...M$_{16}$, the magic header content
begin
    Set EncryptedMessageType $\leftarrow$ B$_{ID}$.Longitude (bits 31...32) $\|$B$_{ID}$.Speed
    (bits 12...13)
    Set MessageType $\leftarrow$ EncryptedMessageType $\oplus$ SecretKey$_2$ (bits 17...20)
    if MessageType = '0001' then
        Set EncryptedMessagePayload $\leftarrow$ B$_{ID}$.Speed (bits 14...16) $\|$
        B$_{ID}$.AccelSet4Way (bit 56) $\|$ B$_{ID+K}$.Latitude (bits 24...32) $\|$
        B$_{ID+K}$.Longitude (bits 24...32) $\|$ B$_{ID+K}$ .Speed (bits 12...16) $\|$
        B$_{ID+K}$.AccelSet4Way (bit 56) $\|$ B$_{ID+2K}$.Latitude (bits 24...31)
        Set ReceivedMessageAuthenticationCode $\leftarrow$ B$_{ID+2K}$.Latitude (bit 32)
        $\|$ B$_{ID+2K}$.Longitude (bits 24...32) $\|$ B$_{ID+2K}$.Speed (bits 12...16) $\|$
        B$_{ID+2K}$.AccelSet4Way (bit 56) $\|$ ... $\|$ B$_{ID+8K}$.Latitude (bits 24...32)
        $\|$ B$_{ID+8K}$.Longitude (bits 24...32) $\|$ B$_{ID+8K}$.Speed (bits 12...16) $\|$
        B$_{ID+8K}$.AccelSet4Way (bit 56)
        # If any of the required fragments is lost, the process returns to the
        embedded message detection (Algorithm 3)
        # Check MAC
        Set MessageAuthenticationCode $\leftarrow$ HMAC(Hash=SHA-1,
        SecretKey$_1$, EncryptedMessagePayload)
        if MessageAuthenticationCode = ReceivedMessageAuthenticationCode
        then
            Set MessagePayload $\leftarrow$ EncryptedMessagePayload $\oplus$ SecretKey$_2$
            (bits 21...56)
```

Algorithm 4: Revealing Algorithm

5.8 Summary of the chapter

In this Section, a mechanism that enables any vehicle to report the misbehavior produced by other vehicles is presented. In order to promote that the report passes unnoticed to other vehicles (and, specially, to the reported one), steganographic techniques have been adapted to this specific context.

Chapter 6

Vehicular-enhanced electronic notification protocol

The electronic notification is a process that enables the fast delivery of a given official information to its intended receiver. However, current notification mechanisms cause offenders to be aware of the punishment long after the offence. Because of that, the Spanish Law 30/92 enables using "new mechanisms based on the upcoming data transmission technologies that speed up the process while respecting the underlying data authenticity requirements" [1]. In this way, notifications may be performed in other places different from the receiver's home [35].

Even if the electronic notification could be performed (in absence of delays) in the order of seconds or minutes, the current goal of the Spanish Traffic Authority is to reduce this gap from 45 days to 12 [11]. At the light of these figures, there is room for improvement as the goal should be put on making the notification to be delivered as soon as possible, even within the same trip in which the offence was committed.

Apart from the previous fact, current mechanisms enable that the offender ignores the notification, i.e. she does not accept or reject it. As a consequence, the offender has the practical chance of not being aware of the notification. Such decision may be taken to increase the probability of failure in the process, typically by

[1] Translated from the Spanish, "Medios de notificación distintos a los tradicionales que, sin merma de las necesarias garantías de autenticidad, permitan su agilización mediante el empleo de las nuevas técnicas de transmisión de información, superándose la limitación de la exclusividad del domicilio como lugar de notificaciones".

exceeding the maximum time interval to perform each legal step.

It is expected that the fast notification delivery and the avoidance of the chance for the offender of being unaware of its content will contribute on increasing the educational effect of the punishment. As a consequence, road traffic safety will be improved. One alternative is to deliver the notification to the mobile phone of the offender. However, the use of such devices while driving is forbidden in several European countries (such as Spain) in order to increase the road traffic safety. Thus, there is a need to find a trade-off solution that ensures the fast delivery of the notification while avoiding distractions to the offending driver.

To contribute on this issue, this Chapter describes the proposed electronic notification protocol that enables delivering the offence notification directly to the vehicle. The use of vehicular embedded systems to receive this information seems to be suitable – such devices are at the core of ITS applications, trying to assist the driver in her task. However, for the particular case of road traffic offence notifications, it is necessary to ensure that the legitimate receiver (the offending driver) had available and further accessed to the notification content. Therefore, the concept of non-repudiation is at the core of the proposed mechanism.

This Chapter is structured as follows. A proposal overview is presented in Section 6.1. The considered model is described in Section 6.2, along with the specific security requirements (derived from the legal provisions) that must be taken into account when designing an electronic notification system. Section 6.3 introduces the architecture derived from the previous model. Finally, the proposed protocol is presented in Section 6.4.

6.1 Proposal overview

The proposed protocol enables sending the offence notification to the offending driver through her vehicle. It is executed once the offence has been detected and the notification has already been prepared.

To perform this notification, the vehicular communication channel is used first. Thus, the notification is sent through RSUs. In order to decide which RSUs must send such message, it is assumed that it is possible to estimate the set of potential positions in which the vehicle may be at the notification moment.

For this notification mechanism to be valid, it is necessary to make it compliant with legal regulations. As there is no explicit regulation for such a mechanism, a set of requirements are derived from those imposed to the existing mechanisms. Among these requirements, it is necessary to attest the reception of the notification message as well as the moment in which it is accessed. In this way, neither of these actions may be repudiated. In order to build these attestations, the vehicular devices issue and send the corresponding evidences of availability and access. It should be noted that the second evidence is built on behalf of the intended notification receiver. This action has to be authorized by the notification receiver beforehand. For this purpose, the use of a password is required. From the conceptual point of view, this action enables the vehicle as a suitable place to receive notifications. Nevertheless, this action may only be performed by one person by vehicle. More precisely, as it is not assumed that when the offence is detected, the current driver is identified, the notification will be referred to the designated-as-offender. Therefore, this mechanism is suitable for offences committed by such person.

Due to the unreliability of the vehicular channel, it may happen that any of the transmitted data gets lost. In order to countermeasure this fact, each message is repeated several times. For consistency with contribution C2, such a simple repetition scheme has been preferred against other approaches based on error correction codes (recall Section 5.6.1). Despite such repetition, some executions may still fail. For these situations, the use of a resilient channel is adopted between the vehicle and the notifying entity.

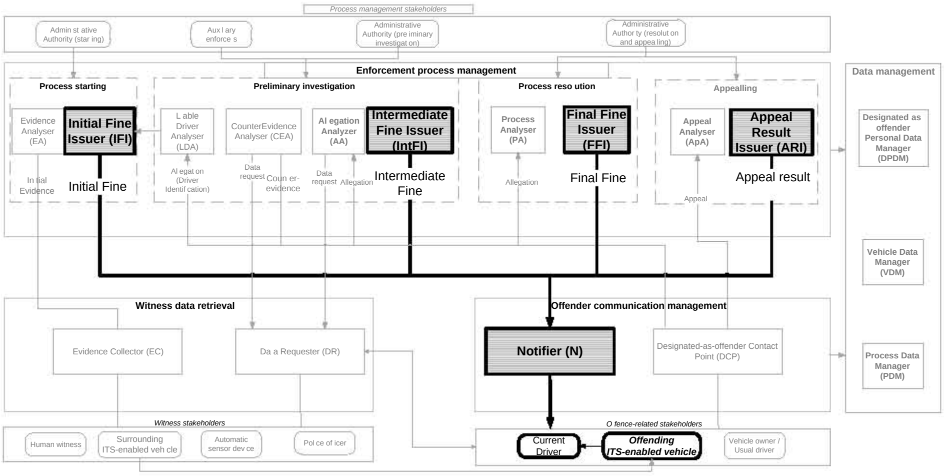

Process management stakeholders
Admin st ative Authority (star ing)
Aux l ary enforce s
Administrative Authority (pre iminary investigat on)
Administrative Author ty (resolut on and appea ling)
Enforcement process management
Process starting
Evidence Analyser (EA)
Initial Fine Issuer (IFI)
In tial Evidence
Initial Fine
Preliminary investigation
L able Driver Analyser (LDA)
Al egat on (Driver Identif cation)
CounterEvidence Analyser (CEA)
Data request
Coun er-evidence
Al egation Analyzer (AA)
Data request
Allegation
Intermediate Fine Issuer (IntFI)
Intermediate Fine
Process reso ution
Process Analyser (PA)
Allegation
Final Fine Issuer (FFI)
Final Fine
Appealling
Appeal Analyser (ApA)
Appeal
Appeal Result Issuer (ARI)
Appeal result
Data management
Designated as offender Personal Data Manager (DPDM)
Vehicle Data Manager (VDM)
Process Data Manager (PDM)
Witness data retrieval
Evidence Collector (EC)
Da a Requester (DR)
Offender communication management
Notifier (N)
Designated-as-offender Contact Point (DCP)
Witness stakeholders
Human witness
Surrounding ITS-enabled veh cle
Automatic sensor dev ce
Pol ce of icer
O fence-related stakeholders
Current Driver
Offending ITS-enabled vehicle
Vehicle owner / Usual driver

Figure 6.1: Parts of the entities model of the enforcement process related to the proposed notification mechanism

6.2 Model

In this Section, the considered model is presented. For this purpose, the entities at stake as well as the different ways in which they may interact are introduced in Section 6.2.1. Afterwards, the security requirements derived from the legal provisions are presented in Section 6.2.2. The implications of the determination of the responsible person in the notification process are discussed in Section 6.2.3. Finally, the working assumptions are presented in Section 6.2.4.

6.2.1 Participant entities

The parts of the entities model (proposed in Chapter 4) related to the mechanism presented herein are highlighted in Figure 6.1. Thus, there is an entity that creates the message to notify (one of the fine issuers or the Appeal Result Issuer) which delegates on another entity (the Notifier) to deliver it to the offender. In the proposed mechanism, the offender is reached through the human-machine interface from her ITS-enabled vehicle.

As the model should serve as a guide to understand the world, and the restrictions that should be taken into account to propose a solution, it is necessary to

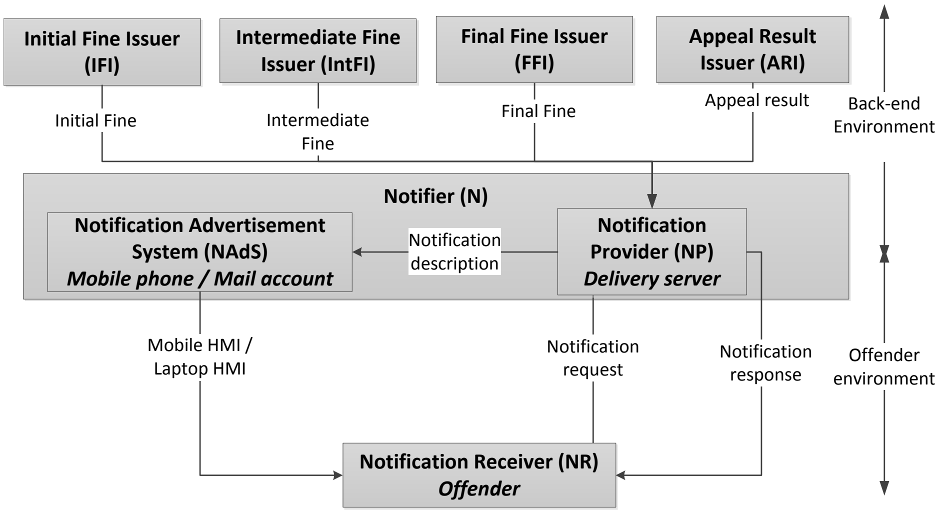


Figure 6.2: Model of current electronic notification mechanisms

use the most specific model that is possible. Thus, a refined version of the aforementioned model will be built, based on the underlying notification model that is followed by current mechanisms.

The legal framework for the electronic notification (Royal Decree 1671/2009, recall Section 3.2.1) establishes four mechanisms and their particular requirements. Except from the last one (which is subject to its own regulation), it is possible to identify a common underlying model for the three first types (see Figure 6.2). The DEV, as a specific type of authorized address, is also covered by this model.

Once the message is created by its issuer (Initial/Intermediate/Final Fine Issuer or Appeal Result Issuer, collectively called Message Issuer (MI) from now on), it is made available through a delivery server (Notification Provider, NP). In order to advert the offender of the existence of such notification, an informative message may be sent to her personal cellular phone or traditional e-mail address (in general terms, *Notification Advertisement System*, NAdS). Both NP and NAdS are different parts of the Notifier (N) identified in the model proposed in Chapter 4. Once this informative message is read by the user (Notification Receiver, NR), or upon her personal will, the offender may access to the delivery server to fetch the notification.

The process finishes with the notification transfer to the offender.

The communication between these entities is produced in two different environments. The connection between the issuers and NP is done in the context of the Traffic Authority infrastructure. On the other hand, NP, NR and NAdS are connected through mobile (i.e. cellular-based or Internet) communication technologies.

Based on this notification-specific model, two refinements will be made over it to better fit to the technical context considered in this thesis. Figure 6.3 shows the definitive model after the mentioned modifications. First, the Notification Advertisement System (NAdS) has been removed, as it is intended to provide the receiver with an informative message regarding the notification existence. This message contributes to make the offender be aware of the notification, thus giving her an appropriate amount of time to take a decision on the notification. As the decision has to be taken as soon as possible in the proposed context, this message is not necessary anymore.

The second refinement is related to the Notification Receiving System (NRS), which is included to alleviate the interaction required by NR. As NR is indeed the actual offender while he/she is driving, its active participation in the protocol should be minimized. In a broad sense, the NRS acts *on behalf of* the NR for the task of receiving the notification. This idea gathers the *interceptor* concept proposed by Robinson [64].

It must be noted that, from a conceptual point of view, the NRS should be considered to be a part of the Notifier from the model proposed in Chapter 4. In other words, it is one of the components in charge of delivering the message between the issuer and the receiver, so it should be taken as part of the Notifier with respect to the legal provisions. In other words, both NP and NRS are notification entities (see Figure 6.3) and they must both comply with the corresponding regulation.

In this situation, the specific model defined so far is not different to the general enforcement model (recall Figure 6.1), but instead it gives a complementary vision

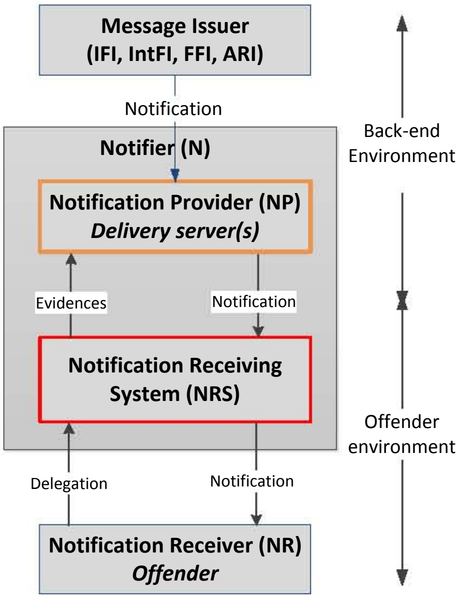


Figure 6.3: Model considered for the vehicular-enhanced notification model

of the same system. NRS deserves special attention, as it is part of the Notifier but it is between the Notification Provider and the Notification Receiver. It may be seen that there are is one equivalent entity in the general model – the Offending ITS-enabled vehicle. The way in which the vehicle may practically become the NRS will be explained in Section 6.3. Therefore, given that both models are complementary, only the specific model will be taken into consideration in the following.

Identified interaction models

In order to access to the notification, there is a request-response exchange between NR and N. Based on the described legal notification mechanisms, there are two models to perform such interaction – *push* and *pull*. In the push model, N sends the notification and, afterwards, NR sends the receipt that attests its access to the content. In the pull one, NR checks periodically if there exists some pending notification. The push model is followed by the e-mail address, whereas the authorized address and the access to the notifier site follow the pull one.

6.2.2 Security requirements derived from the legal framework

Taking into account the general legal framework and the specific issues presented in Section 3.2.1, it is possible to derive a set of requirements that may be fulfilled by the proposed mechanism. Table 6.1 summarizes such requirements, which are referred to as Req$i$. In this Table, the notified message is noted as M.

Requirement	**Description**	**Legal source**
Req1	Non-repudiation of receipt: NP must be aware of the moment in which NRS has received M.	Art. 77.2 Law 18/2009
Req2	Non-repudiation of delivery: N must be aware of the moment in which NR accessed to M.	Art. 77.2 Law 18/2009 (Art 7.2 Order PRE-878-2010)
Req3	Authenticated access control to NRS: Only NR must be able to use (i.e. access, enable as notification place) NRS.	Art. 35.2 R.D. 1671/2009 (Art. 38.1 RD 1671-2009)
Req4	Availability of the notification system: Both NP and NRS must be permanently available to manage M.	Art. 9 Order PRE-878-2010 (Art. 38.1 RD 1671-2009)
Req5	Physical access control: Both NP and NRS must have physical access control mechanisms.	Art. 8 Order PRE-878-2010
Req6	Synchronization: NP and NRS must be synchronized.	Art 7 Order PRE-878-2010
Req7	Message authentication: NR must be able to verify that M was created by MI.	Art 5 Order PRE-878-2010
Req8	Confidentiality of M: M must only be available for MI, NRS and NR.	Art. 6 Order PRE-878-2010
Req9	Integrity of M: It must be possible to determine whether the message M received by NR is the same as the one issued by MI.	Art 5 Order PRE-878-2010

Table 6.1: Summary of requirements for the vehicular-enhanced notification protocol

The set of requirements Req1–Req6 are referred to the notification system, whereas Req7–Req9 are related to the notified message M.

The non-repudiation of receipt (Req1), as well as the non-repudiation of delivery (Req2) are directly derived from Law 18/2009. In both cases, there is a need to have a temporal attestation – in the first case, of the moment in which M was received, and in the second one, of the moment of access to M's content. Such need imposes that there is a global synchronization between all elements of the notification system (Req 6). One important issue is that the attestation must reflect that NR accessed to the content. Such need is the basis for Req3, where authenticated access control is required over NRS – the part of the notification system related to NR. This protection is completed with physical measures (Req5) that may contribute to ensure the permanent availability (Req4).

Concerning the data security, NR must be able to determine if the received notification is authentic. Thus, it must be possible to verify that it was issued by the legitimate entity (Req7) and that it has not been modified since its creation (Req9). Furthermore, it is necessary to avoid third parties to have access to such notification (Req8). According to Order PRE-878-2010, if NP is an external service provider, it should not be able to access to the notification. For the sake of generality, this requirement has been adopted for the proposed mechanism.

6.2.3 Implications of the personal responsibility in the notification process

According to Law 18/2009 [6], the responsible person of a given offence is the one that actually committed it. However, there are several situations that require a special procedure. In case of minors (i.e. persons under the legal age for driving) that are caught when driving, tutors and parents will be also responsible. Concerning motorbikes and any other transport that requires the use of helmets, the driver will be responsible in case that passengers are not wearing them. In those traffic offences in which the car was not stopped, the person identified by the vehicle owner[2] as the usual driver will be responsible, except if she nominates another person or the car had been stolen. If there is no usual driver defined, then the vehicle holder may nominate other person as the driver in the moment of the offence. The vehicle holder will be always responsible for those offences related to the vehicle documentation or maintenance status. Parking offences will be assigned to the vehicle holder (or its short-term tenant, if it exists), except if a usual driver exists or another person is nominated.

The aforementioned considerations are related to the responsible person for an offence, and thus they indicate *who* must receive the notification. Due to the legal nature of this process, it is necessary to send this notification in such a way that its intended receiver is able to gather it. Once the offender has been identified, the notification may be sent. If this person has a suitable place in which he/she is able to get such message[3] to receive such message, it must be sent to this place [6]. Taking into account the considered model (Figure 6.3), NRS is intended to be the aforementioned suitable place. For this purpose, NR must enable NRS as such a place at the beginning of the trip.

6.2.4 Working assumptions

There are six working assumptions in the considered model. Three are related to the vehicular devices, two to the background environment, and one affects to RSUs.

Concerning the vehicular devices, the first assumption is that its HSM has MI's public key certificate preloaded, as well as that from its corresponding issuer. In this way, it is able to verify MI digital signatures. Secondly, the HSM obtains the public key certificate of the RSU at stake through the WAVE Service Announcement message [8]. It is useful to send encrypted messages to the RSU whenever required. Thirdly, the vehicular devices has to perform a set of unavoidable operations at

[2] According to the legislation, the figure of the vehicle holder is equivalent to the long-term tenant. For the sake of brevity, in this discussion only the term vehicle holder will be employed.

[3] Law 18/2009 refers to this point as "lugar cierto de notificaciones", where all traffic-related administrative bodies may send the different messages [6].

the moment in which the engine is started up. Particularly, in case that there are previous notifications, they will be presented at this moment.

Regarding the background environment, it is assumed that it is possible to determine the set of potential locations in which a vehicle may be after a given time after the offence has been detected. In this way, it is possible to deliver the notification message only to the potential locations, thus reducing the impact of this operation. On the other hand, the message issuer knows, at the beginning of the notification process, the pseudonym of the offending vehicle. More specifically, it is assumed that it knows the pseudonym in use at the moment of the notification, apart from the pseudonym at the moment of the offence, which is also assumed to be known. In order to fulfil this assumption, three alternatives may be taken. First, it may be assumed that the pseudonym has not changed between both moments. However, it reduces the applicability of the proposal to such situations, which require a significant processing speed by the Authority. Second, vehicles may be able to receive packets to one of its n recent pseudonyms. Furthermore, in the interval between the offence and the notification, less than n pseudonyms have been used. Such decision is convenient to avoid routing problems [65]. Third, the short-lived pseudonyms may have a validity period (e.g. only valid for Feb, 3rd, 2011, from 19:00 to 20:00). For the purpose of this notification protocol, the second alternative is chosen although the third one is also suitable.

Finally, RSUs are able to contact the certification authority to know the status of a given certificate. On the other hand, such authority offers a service to determine whether two pseudonyms belong to the same entity, without revealing the associated real identity.

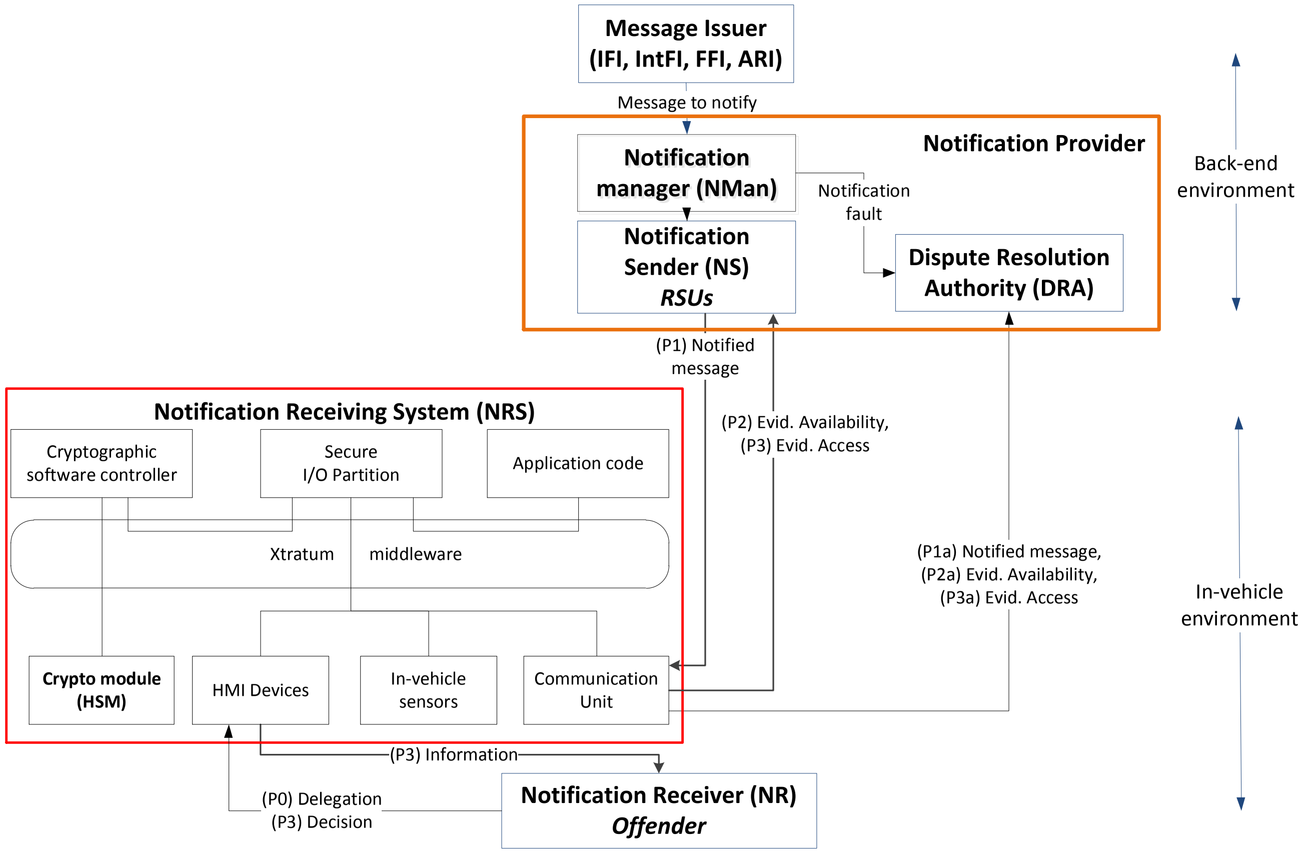


Figure 6.4: VANET-enhanced notification architecture

6.3 Architecture

Based on the model presented in Section 6.2, the architecture considered in this work is shown in Figure 6.4. There are two environments considered in this architecture, namely the back-end environment, and the in-vehicle one. Each one is introduced below.

6.3.1 Back-end environment

There are four entities in the back-end environment, namely the Message Issuer (MI), the Notification Manager (NMan) the Dispute Resolution Authority (DRA) and the Notification Sender (NS). The latter will be presented in Section 6.3.3 as it is not purely from this environment, but it is shared with the vehicular one. Concerning the remaining ones, MI is the entity that creates the message (i.e. the notification), and sends it to NMan for delivery. It is trusted to create notifications of offences that have been detected by the Traffic Authority, ensuring the confidentiality of the data at stake.

The NMan is in charge of contacting the appropriate Notification Senders (i.e. RSUs) to make the notification arrive to the vehicle. For this purpose, it estimates the set of potential positions of the offending vehicle based on its location when the offence was committed and the time gap between the offence and the notification.

Concerning the DRA, it is in charge of performing the notification if it has not been successfully done through RSUs. The name is inspired on the conceptual task – it enables determining whether the failure of the notification through the vehicular channel was due to the channel itself or a malfunction of the vehicular devices.

6.3.2 In-vehicle environment

The in-vehicle environment contains the NRS, which is internally structured as proposed in the OVERSEE project (see Section 2.2.4). Particularly, four components will be at stake, namely the Secure Application Environment (SAE), the Hardware

Security Module (HSM), the On-Board Unit (OBU) and the Human-Machine Interface (HMI). The SAE contains the application code, which is in this case in charge of the processing activities of the vehicle in the notification process. The HSM performs the cryptographic operations, whereas the OBU transmits the information to and from the vehicle. The HMI enables the linkage between the NRS with the Notification Receiver (NR), which is the intended recipient of the notification at stake.

Given that not all NRS components are trusted (particularly, the OBU and the HMI are not protected), the whole NRS component may not be fully trusted for receiving the notification and sending the corresponding evidences when required.

Enabling NRS to receive notifications for NR

One of the needs imposed by the legislation is that NRS must be a suitable place for NR to receive notifications (recall Section 6.2.3). In other words, from NRS' viewpoint, it is necessary to ensure that NR acknowledges that it is such a suitable place for this purpose. In order to solve this issue, one approach is to require an electronic credential to be inserted at the beginning of the trip. Such credential may be a physical one (such as the national identity card or the electronic driving license) or a logical one (a password). It should be noted that such usage has two different implications from the theoretical point of view. First, NRS is able to authenticate NR. Second, this action of inserting a credential may be seen as an authorization from NR, thus enabling NRS as a possible place to receive notifications.

There are two considerations in order to decide between physical or logical credentials. Concerning the robustness, a physical credential is more convenient as it usually requires not only the physical token (e.g. a card) but also some private information, which is indeed a logical credential. However, concerning the short-term applicability, a logical credential is more suitable in that it does not require installing additional hardware. In order to ensure the practical viability of the proposal in the short term, the use of a logical credential is selected.

Using a password has a negative impact on the utility of the proposed mechanism. Thus, if the HSM has to determine whether the introduced password is correct, there is a need to install such password in the device prior to this process. As a result, only one person per car will be able to perform this authentication. This person will be the designated-as-offender (i.e. vehicle holder or its usual driver). This restriction could be relaxed in such a way that more than one password could be pre-loaded, each one associated with one of the frequent drivers of the car. However, in any case this decision requires that such pre-loading operation is performed beforehand.

It should be noted that this action is not transferred to the infrastructure. In this way, the chance of tracking (i.e. determining the path followed by a given person) as a consequence of this action is countered.

6.3.3 Connection between environments

There are two different types of connection between the aforementioned environments, each one having different communication features. The first one (called *mobility* context) is used while the vehicle is on the road, whereas the second one (*static* context) is used when the vehicle is stopped for some time, such as the home garage.

In the mobility context, the communication is established between RSUs (Road-Side Units) and the vehicular OBUs already introduced in the in-vehicle environment. RSUs are static nodes that are placed aside the roads. They are managed by the Authority, and thus they are assumed to reliably perform their communication tasks. RSUs are intended to offer a set of services to passing by vehicles. For this purpose, they are connected to backbone servers that act as service providers.

The communication channel in the mobility context is based on a wireless short-range technology called DSRC (Dedicated Short-Range Communications) which has a nominal range of 1 km. Due to the very nature of the wireless medium, the channel is inherently unreliable (i.e. packets may be lost). Thus, timeliness may only be achieved by means of deadlines, but this mechanism is not able to ensure that the fairness property is fulfilled in unreliable channels [66].

With respect to the static context, the communication takes place between the vehicular OBU and DRA. This connection may be wireless (e.g. through the at-home Wi-Fi network) or even wired (e.g. for electric vehicles during the recharge process). In any case, this context is physically bounded, which is an inherent protective measure. Therefore, such connection is considered as resilient (i.e. packets will arrive to its destination after a finite, but unknown, amount of time).

6.3.4 Selection of the interaction model

Once the implementation of each of the considered entities is defined, it is possible to determine which interaction model is more suitable among those identified in Section 6.2.1.

The push model imposes that NS (i.e. the RSU) proactively sends the notification to NRS (i.e. the in-vehicle computation device). For this purpose, it is necessary to know the location of such vehicle. It should be noted that the offence place was already known – once the offence was detected at the beginning of the enforcement process, its place was recorded within the initial evidence (recall Section 4.4). Based on this information, it is possible to estimate the set of potential locations in which the vehicle may be, considering the time interval between the offence and the notification. Thus, there is no need to *track* the vehicle movement, which would threat the driver privacy.

On the other hand, the pull model requires that the vehicle periodically requests for new notifications to the RSU. It must be noted that this would cause non-offending vehicles to perform such unnecessary requests. As the vehicular network has to deal with safety-related ITS applications, saving bandwidth should be put as a critical design goal. Furthermore, this periodic action would require an authentication against RSUs, which could enable tracking. For these reasons, the interaction model selected for the unreliable channel is the push one.

Concerning the resilient channel between NRS and DRA, the selected interaction model is the pull one. In this case, the natural interaction is that at the beginning of the periodic connection, NRS authenticates itself against DRA. As a result, the DRA knows when NRS is available, and then it may proceed to send all the information related to NRS. It should be noted that this connection could be re-used with other entities of the Traffic Authority to solve other periodic processes, such as credential renewal, tax revisions, etc.

6.3.5 Threat model

In this Section, the different threats related to each element in the architecture are described. It must be noted that four elements (Message Issuer, Dispute Resolution Authority, RSUs and the back-end communication channel) are assumed to be trusted for the purpose of this mechanism[4]. Therefore, there are no threats related to these elements. The following subsections describe the corresponding threats for the remaining elements.

Compromise of VANET communication channel

The VANET communication channel may be eavesdropped by any other entity in range. Moreover, new messages may be injected in the conversation and existing ones may be altered.

The channel may be filled with (potentially useless) messages. However, we assume that Denial-of-Service (DoS) attacks have been already addressed (for example, using the LEAVE protocol [67]).

[4] This assumption does not mean that such entities are fully free of threats. However, in case that they exist, they do not interfere with the mechanism presented herein.

It must be noted that an intrinsic threat is posed by the channel unreliability, which may cause any sent data to be lost.

Compromise of HMI devices

OVERSEE does not offer any kind of security service to protect against alteration of the HMI devices or their connection networks. Thus, they rely on their own physical countermeasures.

For the context of this contribution, the threat of compromise of HMI devices is not considered. This threat may be caused by a malicious manipulation or by an accidental malfunctioning operation. The relevance of this threat in this context is that the HMI may report that the notification was accessed by the driver, but actually it did not occur. Even if this threat is feasible, its solution will require the development of software-hardware mechanisms that ensure its proper operation. The design of such mechanisms is out of the scope of this contribution.

Compromise of OBUs

There are two main threats related to the OBU and its connection network – its complete blockage and its selective manipulation. For the context of this contribution, both threats must be assumed as possible.

Regarding the first threat, it has been extensively studied in the e-toll field. A case study may be the Toll Collect system which is currently running in Germany. In order to detect this threat, control bridges are placed along the road. Each vehicle is scanned, and it is determined whether or not it is subject to toll payment. If it is the case, the bridge communicates (through DSRC) to the OBU to determine whether the vehicle is participating in the automatic toll collection system and if the OBU is properly switched on. If a vehicle subject to toll is not emitting an infrared signal, it has either logged on manually or is in violation. To clarify this, the number plate of each vehicle is photographed with an infrared camera and compared with the logged on number plate at Toll Collect headquarters. If it is discovered that the vehicle is not manually logged on, the information is forwarded to BAG authorities and an administrative fine is issued [68].

With respect to the second threat, it implies that the attacker is able to control the OBU at her own will, intervening this component in a different way depending on the data at stake. Thus, it may avoid sending some message or sending an altered version. Moreover, it may avoid sending data outside the vehicle or just sending some modified information.

6.4 Protocol definition

The notification at stake is sent by the Message Issuer (MI) to the Notification Receiver (NR). However, none of these entities will have a direct role within the non-repudiation interaction. On the one hand, the MI is assumed to be trusted to create the notification itself, and its communication with the Notification Sender (NS) through the Notification Manager (NMan) is reliable. Therefore, there is no need to implement a non-repudiation protocol between these entities. On the other side, by design of the model, the NR delegates into the Notification Receiving System (NRS) for receiving data. As in the previous case, there are not non-repudiation issues between these entities.

Taking into account the previous considerations, the only step in the whole notification transfer process that may be challenged is the communication between NS and NRS. Such protocol is designed in this Section.

6.4.1 Data structures

Apart from the notification itself, whose transference is the main goal of this protocol, there are two additional data structures, namely the evidence of availability and the evidence of access to the content. Such two structures are derived from the non-repudiation requirements introduced in Section 6.2.2. Tables 6.2, 6.3, and

6.4 show the contents of the notification, the evidence of availability and of access, respectively.

Data group	**Element**	**Size (bytes)**
Offender	Vehicle Identifier	4
	Offender name	30
	Offender identifier	4
Offence and punishment	Description	30
	Date	4
	Place	10
	Time	2
	Issuer name	20
	Offended rule	10
	Punishment	4
	Demerit points	1
Witness	Device identifier	4
Future actions	Legal terms, time interval, explanation on future actions	100
Signature	Signature value	56
	Public key certificate	125
Total	**Size**	**404**

Table 6.2: Contents of the Notification message

The notification contents follow the legal provisions on this regard (see Section 3.2.2). Only two refinements are made over such contents – the postal address is removed (as it is the own vehicle the place of notification) and the digital signature of the issuing Authority is added to ensure the data origin and integrity. Even if the public key certificate of MI is pre-loaded in vehicles, it is also included in the notification to simplify its updating.

Data group	**Element**	**Size (bytes)**
Message	Digest value	32
Availability time	Time mark	4
Signature	Signature value	56
	Public key certificate	125
Total	**Size**	**217**

Table 6.3: Contents of the Evidence of availability message

Data group	**Element**	**Size (bytes)**
Message	Digest value	32
Access description	Time mark	4
	Decision	1
Signature	Signature value	56
	Public key certificate	125
Total	**Size**	**218**

Table 6.4: Contents of the Evidence of access message

The evidence of availability (referred to as *EoA*) is created by the HSM acting on its own behalf. It contains (1) the hash of the received notification and (2) the moment in which it was received. The digital signature of the HSM (using the current pseudonym) over the previous two fields is also contained herein, along with its public key certificate. The evidence of access (referred to as *EoAcc*) is created by the HSM acting on behalf of the notification receiver. Additionally to the fields introduced in EoA, it includes the decision (i.e. accept or reject) that has been taken concerning the notification. Such field is also taken into account when the digital signature is calculated. Such digital signatures are created using the keys associated with the pseudonym that appears in the notification. The sizes of public key certificates and digital signatures are taken from the IEEE 1609.2 standard [8].

6.4.2 Notation

This Section describes the notation in use in the protocol specification. Concerning the data structures, they will be noted as $Notif$ for the notification, *EoA* for the evidence of availability and *EoAcc* for the evidence of access. With respect to the cryptographic operations, public key encryption ($\mathrm{E}_{X(t)}(\mathrm{M})$) and its corresponding decryption ($\mathrm{E}^{-1}_{X(t)}(\mathrm{M})$), as well as digital signatures ($\mathrm{S}_{X(t)}(\mathrm{M})$) and their verifications ($\mathrm{S}^{-1}_{X(t)}(\mathrm{M})$) are in use. In these cases, $X(t)$ refers to the pseudonym of entity X at time t, which has a public-private keypair used for cryptographic operations. For example, in the encryption process the public key will be used whereas the private one is employed in the decryption operation.

6.4.3 Protocol specification

The protocol consists of three main steps – sending (1) the notification to the vehicle, (2) the evidence of availability from the vehicle once the message has been successfully received and (3) the evidence of access from the vehicle once the driver has accessed to its contents. However, both the vehicular network failure and the OBU compromise may become an obstacle to the regular protocol development and thus they must be properly managed.

Algorithm 5 describes the data exchange between the different entities. The process starts (step 0) with NR enabling NRS to be the place in which notifications addressed to her may be received. For this purpose, a password is introduced into the NRS's HSM.

Once the offence is detected, MI prepares the notification and sends it to the NMan, along with its hash, the pseudonym in use of the HSM (at the time of the offence), and the time of the offence $\mathrm{t}_{offence}$ (step 1a). Once NMan has estimated the set of potential positions of the vehicle, it sends the notification to the corresponding Notification Senders (i.e. RSUs)[5] . They will try to send this message to the OBU, although at most only one will be able to achieve it (step 1b). It should be noted that also the public key certificate and the signature value are sent encrypted. The confidentiality of the public key certificate ensures that other vehicles will not be able to guess the nature of the message (as the amount of types

[5] For the sake of clarity, in this Section the terms *RSU* and *Notification Sender* will be used interchangeably.

of messages that such entity may send to vehicles is really reduced).

The OBU transfers this message through the SAE to the HSM, which decrypts the message using the private key associated to the pseudonym in use, and verifies the notification signature using the public key certificate of MI (step 2a). If such verification is successful, the evidence of availability is prepared and sent to the RSU that sent the notification[6] (step 2b). For this purpose, a hash function is applied over the notification and a time mark is obtained from the HSM internal time source. All these data are signed using the private key associated with the pseudonym in use. Such signature is verified by the RSU (step 2c).

The notification message is then presented to the driver by means of the Human-Machine Interface (HMI) (step 3a). The driver may take a decision on the notification, which will be employed to prepare the evidence of access (step 3b). Such decision may be explicit (i.e. an action of accepting or rejecting the message in an idle driving time) or implicit (i.e. a pre-defined action established by the driver, for example by means of policies). Such evidence is sent to the aforementioned RSU (step 3c), which again verifies the signature (step 3d). Furthermore, it also determines whether the received evidences are semantically correct. Thus, the digest values must be the same as that received in step 1b and the respective time marks must be coherent (i.e. the evidence of availability must be prior to the evidence of access, and both dated before the current time).

The previous data transmissions with RSUs are developed through the vehicular communication. For this purpose, each of the steps is repeated a number α of times to counter the eventual data loss caused by the unreliability of this channel[7]. Section 8.3.1 analyzes possible values for such parameter. An optimization of this mechanism is to avoid sending α retransmissions, by incorporating an acknowledgement mechanism. In this way, once the message is received, the remaining

[6] The special situation in which the NRS is not enabled as a suitable place to receive notifications is discussed at the end of this Section.

[7] Such repetition is transparent to the driver. Thus, re-sending the evidence of access does not require taking a decision for each repetition.

repetitions would be avoided. Nevertheless, the reduced size of messages (which involves a short transmission time) along with the fact that repetitions may be sent without delays (if enabled by the network usage), make that a regular acknowledgement message be impractical – it could be sent once all retransmissions have been already sent.

Both the evidence of availability and of access are expected to be sent to any of the involved RSUs (more specifically, to the RSU from which the vehicle received the notification message) after a realistic amount of time. As an example, it is not reasonable to wait one hour to receive these evidences, as the vehicular mobility imposes that after such an interval the vehicle will be surely out of the RSUs range. Thus, after a reasonable interval (see Section 8.3.1 for an illustration of the size of this interval), all RSUs contacted in step 1b send the results on their verification of the evidences (both the signature verification and semantic checks). Those RSUs that have not received any message simply send a $false$ value.

After receiving these values from all RSUs, the NMan establishes if the process has been successfully finished. Thus, if both evidences have been verified by one RSU, the notification is adequately performed. If it is not the case, then NMan contacts DRA (step 3f), sending both the notification, the pseudonym in use by the HSM and the time $\mathrm{t}_{offence}$ (already received by NMan in step 1a).

The process followed by DRA (Algorithm 6) starts after a mutual authentication between HSM and DRA. It should be noted that the HSM never reveals its real identity to DRA, but instead it uses one pseudonym to authenticate. DRA contacts the certification authority to determine if the presented pseudonym is related to the one sent by the NMan. If it is the case, then the process starts (step 1 in Algorithm 6) by sending the notification message as well as the time of the notification $\mathrm{t}_{offence}$. Such time mark is necessary to enable HSM retrieving the pseudonym that was in use at the time of the offence. Using such pseudonym (more specifically, its associated public key), it is possible for HSM to decrypt the notification. Moreover,

```
begin
    (0) NR → HMI → SAE → HSM : password (HSM)
    # Once the offence has been detected and processed
    (1a) MI → NMan → RSU-set : $E_{hsm(Toffence)}$ (Notif), $hsm(Toffence)$,
    $t_{offence}$, $t_{notif}$, Hash(Notif)
    # Message (1b) is re-sent $\alpha$ times by each RSU in RSU-set
    (1b) RSU → OBU → SAE → HSM : $E_{hsm(Toffence)}$ (Notif)
    (2a) HSM → SAE: notifAuth = $S^{-1}_{MI}(E^{-1}_{hsm(Toffence)}$(Notif))
    if notifAuth == true then
        # Upon request from SAE, the HSM creates the evidence of
        availability
        (2b) HSM → SAE → OBU → RSU : $E_{RSU}$ (EoA)
        (2c) RSU : evidAuth = $S^{-1}_{hsm(Toffence)}(E^{-1}_{RSU}$(EoA))
        (3a) SAE → HMI → NR : notification data
        # Once the offender has accessed to the notification content
        (3b) NR → HMI → SAE → HSM: Decision
        (3c) HSM → SAE → OBU → RSU : $E_{RSU}$(EoAcc)
        (3d) RSU : evidAvailAuth = $S^{-1}_{hsm(Toffence)}(E^{-1}_{RSU}$(EoAcc))
        # RSU establishes the value evidCoherence by comparing both
        evidences each other, as well as the hash value contained in them with
        the value Hash(Notif) received in step 1b
        # Message (3e) is sent by each RSU in RSU-set
    (3e) RSU → NMan : evidAuth, evidAvailAuth
    if (evidAuth == false OR evidAvailAuth == false OR evidCoherence ==
    false) for all RSUs in RSU-set then
        (3f) NMan → DRA : $E_{hsm(Toffence)}$ (Notif), $hsm(Toffence)$,
        $t_{offence}$, Hash(Notif)
        # Start the notification process through the DRA (Algorithm 6)
```

Algorithm 5: Notification process over the vehicular channel

```
begin
    # This process starts after a successful mutual authentication between HSM and DRA
    (1) DRA → OBU → SAE → HSM : $E_{hsm(Toffence)}$ (Notif), $t_{offence}$
    (2a) HSM : notifAuth = $S^{-1}_{MI}(E^{-1}_{hsm(Toffence)}(Notif))$
    # Upon request from SAE, the HSM creates the evidence of availability
    (2b) HSM → SAE → OBU → DRA : $E_{DRA}$ (EoA)
    (2c) DRA : evidAuth = $S^{-1}_{hsm(Tnotif-dra)}(E^{-1}_{DRA}(EoA))$
    if evidAuth == false then
        Repeat the process from the beginning. If the result is the same,
        DRA takes evidence on this situation and contacts the Traffic
        Authority to call the vehicle for revision of its devices
        The notification should be performed using the
        non-vehicular-enhanced mechanisms
    if notifAuth == true then
        (3a) SAE → HMI → NR : notification data
        # Once the offender has accessed to the notification content
        (3b) NR → HMI → SAE → HSM: Decision
        (3c) HSM → SAE → OBU → DRA : $E_{DRA}$(EoAcc)
        (3d) DRA : evidAvailAuth = $S^{-1}_{hsm(Toffence)}(E^{-1}_{DRA}(EoAcc))$
        # DRA establishes the value evidCoherence by comparing both
        evidences each other, as well as the hash value contained in them with
        the value Hash(Notif) received at the end of Algorithm 5
    if evidAvailAuth == false OR evidCoherence == false then
        # The vehicular-enhanced electronic notification is not successfully
        completed
        Repeat the process from the beginning. If the result is the same,
        DRA takes evidence on this situation and contacts the Traffic
        Authority to call the vehicle for revision of its devices
        The notification should be performed using the
        non-vehicular-enhanced mechanisms
```

Algorithm 6: Notification process performed by DRA after a failure of the vehicular channel

using MI's public key, it verifies the notification signature (step 2a). The following steps (2b to 3d) are the same as those described in Algorithm 5. The only difference is that even if the notification signature was not successfully verified, the evidence of availability is prepared and sent to DRA as a means to inform this entity of the situation. Only if the signature is verified the notification is presented to the notification receiver.

If DRA detects that either the signature of any of the evidences is not correct, it may repeat the process from the beginning. As the time available for this resilient connection is several orders greater than the time to perform this exchange, it is possible to perform this repetition (as opposed to what happened in the vehicular environment). If the result is the same, then it is assumed that the in-vehicle platform is not working properly. In such a case, the notification protocol is failed and it should be performed using other traditional mechanisms. Furthermore, DRA calls for maintenance to the affected vehicle.

One important difference is that the time required to access to the notification may be greater than that in the vehicular connection. As an example, consider that the resilient connection is established in the parking of the offender's home. It may happen that the notification is received once after the offender has left the car. In such a situation, the notification will be accessed the next time the offender introduces the password. Particularly, in order to prevent the driver ignore the notification, in case that no decision is taken on this issue, the SAE determines that it has been rejected and creates (autonomously) the evidence of access including such decision. Even in this situation, it may happen that the offender *never* introduces again the password. It may happen, for example, if the vehicle is sold. In such scenario, the reason for the protocol not finishing successfully is not related to the malfunctioning of the in-vehicle devices or the passive behavior from the notification receiver – the only reason is that the vehicle is not a suitable notification place anymore. To prevent DRA reaching a deadlock, a timer must be set. The definition of the waiting time highly depends on the usage patterns of the vehicle and the frequency of the resilient channel. Thus, for a channel that is usually established at a daily basis, waiting more than two days does not seem to be reasonable. A policy to determine such interval is left to future work. It should be noted that this timer has a different purpose than the 10-days timer established by current legislation. If the action that enables the NRS as a suitable notification place (i.e. inserting a password, in the proposed protocol) is set as a prerequisite for the vehicle ignition, then the passive behavior (which was the goal of the 10-days timer) is countered – the next time the offender tries to use the vehicle, she will be forced to take a decision (or the vehicle will autonomously take it on her behalf). The timer defined in this protocol is intended to prevent unnecessary waiting times derived for special situations such as the one described above.

Handling NRSs not enabled to receive notifications for NR

The proposed protocol is based on the fact that at its very beginning (step 0), NR introduces the password that enables NRS as a suitable place to receive notifications. However, it may happen that the vehicle is driven by a person different from the one that has the password pre-loaded in the vehicle. In this case, the vehicle is not a suitable place for receiving notifications. To reflect this fact, the HSM inserts a *void* time mark in the evidence of availability (step 2b of Algorithm 5). This issue is recognized by the RSU, which communicates this fact to the NMan. Based on this information, the NMan determines that it is not possible to perform a vehicular-enhanced notification protocol and it proceeds with one of the existing notification mechanisms.

6.5 Summary of the chapter

In this chapter, a novel electronic notification protocol has been presented. Such protocol is based on the upcoming communication capabilities of vehicles. In this way, the notification may be sent directly to the offending vehicle, thus reducing the time gap between the offence and its punishment. Moreover, in case that the notification is not successfully done, the interacting parties take notice of this situation in order to proceed with other existing notification mechanisms.

Chapter 7

EVIGEN: A protocol for vehicular cooperative EVIdence GENeration

In order to ensure that a punishment is fair, it is necessary to provide the offender with enough elements to defend herself. Nevertheless, for the road traffic enforcement process there is currently no practical mechanism to create these defensive elements that help the driver on attesting its driving behavior or the surrounding circumstances. The low amount of counterevidences presented by offenders, even if around the 36 % of drivers find this punishment system to be unfair, may be seen as an indicator of the lack of a real means for building these supporting elements.

To contribute on this issue, in this Chapter a mechanism to cooperatively create vehicular evidences about the recent driving behavior is presented. This mechanism is applied after the offence notification is received in the computational device of the offending vehicle (as detailed in Chapter 6). Particularly, only the scenario in which the notification is sent to the vehicle through the VANET is considered. The scope of this protocol covers not only the evidence creation but also its verification. Nevertheless, the trustworthiness evaluation of the data provided by such surrounding vehicles is out of the scope. The threat of collusion among vehicles (to give a collective false vision of a given situation) is also out of the scope.

Section 7.1 gives an overview of the proposal. Afterwards, the model and ar-

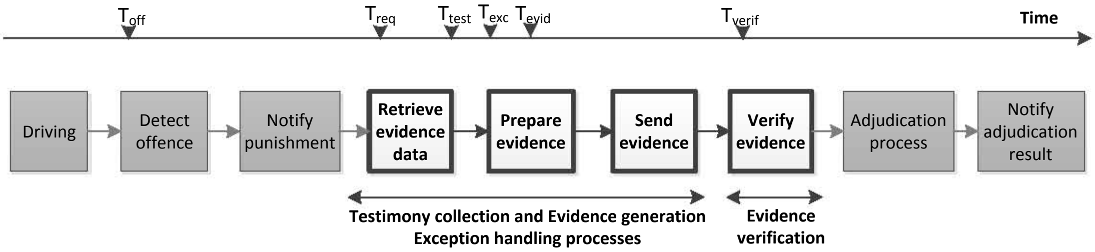


Figure 7.1: Proposal scope within the enforcement process and timeline. Covered steps have been marked in white.

chitecture are presented in Section 7.2 and Section 7.3, respectively. Finally, the protocol is described in Section 7.4.

7.1 Proposal overview

The proposed protocol enables the cooperative creation of evidences that may help on supporting a given claim. In this work, it will be applied to help a driver on defending herself against an unfair punishment. Thus, the protocol is executed after an offence notification is received and its resulting evidence (called *counterevidence* in the proposed enforcement model, see Chapter 4) will be sent to the Authority for evaluation (see Figure 7.1).

Before the purported offence is detected, vehicles are being driven, exchanging status data through VANET *beacons*, i.e. messages containing (among other data) the position and speed of the sender vehicle and which are sent to all one-hop communication neighbours. Once an offence is detected, a fine notification is sent to the offending driver through the computational device of the vehicle. This device analyses the fairness of the received notification. For this purpose, it compares the offence description with its recent behavior, based on the information provided by in-vehicle sensors. If such device finds that the punishment is not fair, it asks surrounding vehicles (*witnesses*) for supporting data that may help on decreasing the fine. Particularly, the one-hop neighbours when the offence was purportedly committed are surveyed. Each of these vehicles may send an estimation (called *testimony*) of the previous *behavior* of the offender. On the other hand, the vehicle requesting testimonies will send its claimed value for the behavior-related variable, along with the list of witnesses that should be sending their testimonies to support the claim. Using such list and the corresponding testimonies, the evidence is built and sent to the appropriate entity in the Authority domain for evaluation.

As vehicles are connected through a wireless network, data may get lost in the communication channel. To deal with this issue, two exception handling procedures are proposed, one for the offender vehicle and the other for witnesses. These protocols are executed over a resilient network, such as an at-home connection. As a difference with contributions C2 and C3, this protocol does not contain any strategy of repeating several times each of the exchanged messages to counter the vehicular network unreliability. This decision aims to avoid the waste of resources for a mechanism which is only fruitful for one person – the offender. In contribution C2, reporting misbehaving vehicles is of the interest of the whole set of drivers, as it contributes on removing them from the roads. On the other hand, contribution C3 is focused on delivering the notification, thus increasing the global speed of the process, which is beneficial for the sustainability of the road traffic administration body.

7.2 Model

This Section describes the considered model for this contribution. Section 7.2.1 introduces the participant entities. Section 7.2.2 describes the requirements that the mechanism has to fulfil. Finally, Section 7.2.3 describes the working assumptions that are taken into account.

7.2.1 Participant entities

The parts of the enforcement process related to this mechanism are highlighted in Figure 7.2. Thus, the Offending ITS-enabled vehicle will perform two different

Element	Symbol	Content / Description
Participant entities	OBU_i	On Board Unit *i*.
	R, R(t)	Requester, using pseudonym R(t) on time *t*.
	W_i, W_i(t)	Witness *i*, using pseudonym W_i(t) in time *t*.
	EM	Evidence Manager.
	HSM_R, HSM_{Wi}	Hardware Security Module of R and W_i, respectively.
	SAE_R, SAE_{Wi}	Sec. App. Environment of R and W_i, respectively.
	Adj	Adjudicator.
	CA	Certification Authority.
Crypto. operations	$\mathrm{S}_{X(t)}$(M)	Signature over 'M' using entity X private key at time 't'. It denotes the message 'M' and its signature value.
	$\mathrm{S}^{-1}_{X(t)}$(M)	Signature verification over the signed message 'M' using entity X public key at time 't'. It represents the result (*true* or *false*) of this operation
	$\mathrm{E}_{X(t)}$(M)	Message 'M' encrypted with entity X public key at time 't'.
	$\mathrm{E}_{X(t)^{-1}}$(M)	Decryption of message 'M' using entity X's private key at time 't'.
Data elements	Cert_E(t)	Public key certificate of entity E at time *t*
	t_{off}, t_{req}, t_{test}, t_{evid}	Time mark of the offence, of the request, of the testimony and of the evidence. Figure 7.1 graphically represents such moments.
	offence-id	Offence identifier given by the road traffic authority.
Data structures	$\mathrm{Beacon}_{R(t)}$	$\mathrm{S}_{R(t)}$(R(t), speed, position, t)
	$\mathrm{Req}_{R(Treq)}$	(part1, part2) where *part1* = $\mathrm{S}_{R(Treq)}$(R(t_{off}), t_{off}), and *part2* = $\mathrm{S}_{R(Toff)}$(offence-id, type), being *type* = position or speed
	$\mathrm{Testim}_{Wi(Ttest)}$	$\mathrm{S}_{Wi(Ttest)}$ (W_i(t_{test}), offence-id, R(t_{off}), [position or speed], t_{test})
	$\mathrm{EvidHdr}_{R(Tevid)}$	$\mathrm{S}_{R(Tevid)}$ (R(t_{evid}), offence-id, claimedValue, t_{off}, $\mathrm{Beacon}_{W1(Toff)}$, $\mathrm{Cert}_{W1(Toff)}$,...$\mathrm{Beacon}_{Wn(Toff)}$, $\mathrm{Cert}_{Wn(Toff)}$, t_{evHdr})
	Evid_{EM}	S_{EM}($\mathrm{EvidHdr}_{R(Tevid)}$ (offence-id), SupportingTestim, t_{evid}) where SupportingTestim ={ $\mathrm{Testim}_{W1(Ttest)}$, ... , $\mathrm{Testim}_{Wn(Ttest)}$ }
Auxiliary functions	contains(data,min,max)	Determines if *data* ∊ [*min*,*max*]. Returns *true* if this condition holds.
	lookupBehRecord($\mathrm{Know}_{Wi(t1)}$(t_1), R(t_2), t_2, type)	Searches whether W_i knows the behavior-related variable according to *type* of vehicle R(t_2) in t_2. Returns such value, or *null* if it does not exist.
	lookupCert(Know_{E1}(t_1), E_2, t_2)	Searches within Know_{E1}(t_1) if Cert_{E2}(t_2) was known. It returns such certificate, if existed.
	findNeighbours(E, t)	Returns *neighbourSet*, the set of vehicles that were known to entity *E* at time *t*. It also outputs the beacons (*beaconSet*) that showed the existence of such knowledge relationship, and the corresponding public key certificates (*certSet*)
	storeTestimony(E,Testim_{E1}(E_2, offence-id), Cert_{E1}(t_{testim}))	Stores the testimony in Know_E(t_{store}), being t_{store} the moment in which the function is invoked and t_{testim} the time of the testimony.
	retrieveTestimony(Know_{E1}(t), E_2, offence-id, t)	Searches within the knowledge set of entity E_1 the testimony of entity E_2 referred to offence *offence-id* in time *t*. It returns such testimony (along with the corresponding public key certificate), if existed.
	checkPseudonymsEntity(E(t_1),E(t_2))	Returns *true* if pseudonyms E(t_1) and E(t_2) belong to the same entity *E*.

Table 7.1: Notation summary

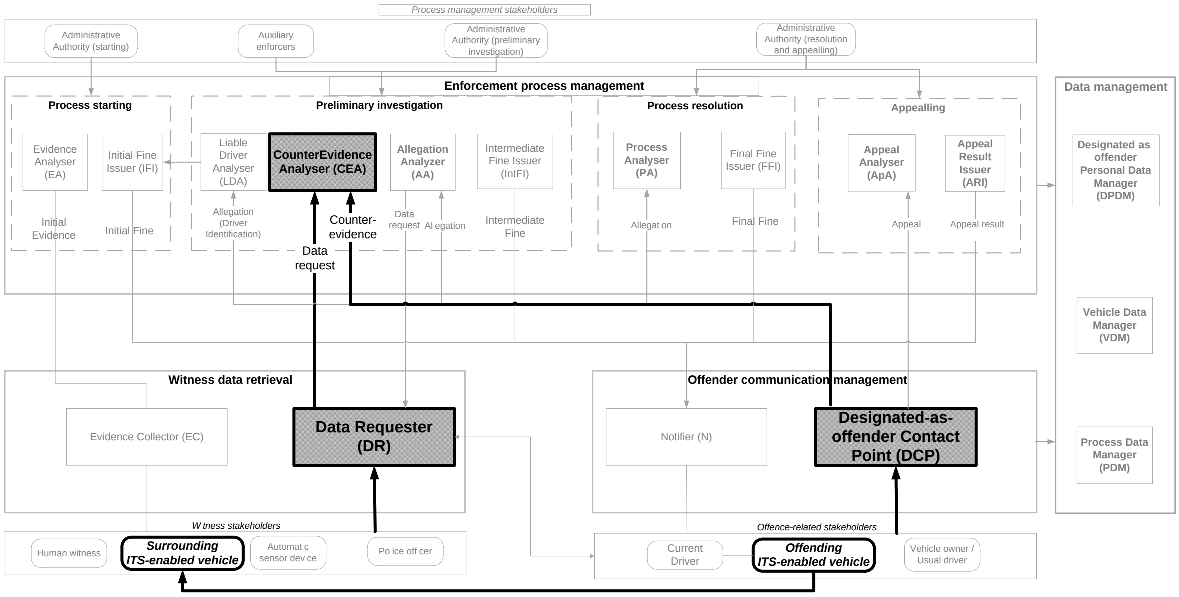

Process management stakeholders
Administrative Authority (starting)
Auxiliary enforcers
Administrative Authority (preliminary investigation)
Administrative Authority (resolution and appealling)
Enforcement process management
Process starting
Evidence Analyser (EA)
Initial Fine Issuer (IFI)
Initial Evidence
Initial Fine
Preliminary investigation
Liable Driver Analyser (LDA)
CounterEvidence Analyser (CEA)
Allegation Analyzer (AA)
Intermediate Fine Issuer (IntFI)
Allegation (Driver Identification)
Counter-evidence
Data request
Data request
Al egation
Intermediate Fine
Process resolution
Process Analyser (PA)
Final Fine Issuer (FFI)
Allegat on
Final Fine
Appealling
Appeal Analyser (ApA)
Appeal Result Issuer (ARI)
Appeal
Appeal result
Data management
Designated as offender Personal Data Manager (DPDM)
Vehicle Data Manager (VDM)
Process Data Manager (PDM)
Witness data retrieval
Evidence Collector (EC)
Data Requester (DR)
Offender communication management
Notifier (N)
Designated-as-offender Contact Point (DCP)
W tness stakeholders
Human witness
Surrounding ITS-enabled vehicle
Automat c sensor dev ce
Po ice off cer
Offence-related stakeholders
Current Driver
Offending ITS-enabled vehicle
Vehicle owner / Usual driver

Figure 7.2: Parts of the entities model of the enforcement process related to the cooperative evidence generation mechanism

actions. First, it will send to the Authority (especifically, the CounterEvidence Analyzer, CEA) its claim on its past behavior. For this purpose, the Designated-as-Offender Contact Point (DCP) will be used as the intermediary of this communication. In this way, the Offending vehicle does not have to care the specific CEA that has to be contacted, which may depend on the internal organization of the enforcement infrastructure.

The second action is to obtain the information (called *testimonies*) from surrounding vehicles. From the logical point of view, this interaction involves that at a certain point in time it is necessary to extract from such vehicles some information. This data is requested directly from the Offending ITS-enabled vehicle to the Surrounding ITS-enabled vehicles. The latter sends the data to the CEA through the Data Requester (DR), which is the entity in charge of retrieving data from witness stakeholders.

Identified interaction models

There are three ways in which the identified entities may interact to perform the counterevidence generation process. They will be referred to as the *centralized* approach, the *decentralized* and the *combined* ones. In the first case, the Offending ITS-enabled vehicle relies on DR (which is seen as a single, central entity) to ask the Surrounding vehicles on behalf of the Offending one, to retrieve their information and to create the counterevidence. In the decentralized approach, it is the Offending ITS-enabled vehicle which asks for the Surrounding vehicle data, retrieves it and builds the counterevidence. In the combined one, it is the Offending vehicle who requests for testimonies, while DR collects them. The Offending vehicle then sends a summary of its expectations on the future counterevidence. Based on this summary, the CEA (which receives such summary along with the data retrieved by DR) compiles the counterevidence and proceeds with its verification and evaluation.

From the enforcement model point of view, the three identified interaction models are suitable. Even if any of them matches exactly the data flows of the enforcement model, all of them respect the definition of the entities and the logical division of their responsibilities. Thus, in all cases DR is focused on retrieving data from witness stakeholders, DCP is the entity that receives data from the offence-related stakeholder (the Offending vehicle, in this case) and CEA focuses on analysing the counterevidence, obtaining data from DR when necessary to perform this evaluation.

7.2.2 Requirements

There are four requirements that must be achieved by the devised solution. Each one is introduced below.

Correctness. The protocol must enable the creation of a behavior-describing evidence *ev* for a Requester vehicle (R). Such evidence must contain one or more testimonies from surrounding Witness vehicles (W_i). The protocol must enable the

Adjudicator *Adj* to validate the aforementioned evidence. For this purpose, the following five conditions must hold:

Condition 1 (supported evidence). *ev* has to contain at least one testimony referred to the offence identifier *offence-id* to which the evidence is related.

Condition 2 (value consistency). Let $testimValue$ be the perception of the behavior-related variable included in a testimony appearing in *ev*. Given that $claimedValue$ is R's claim on that variable, the operation $contains(testimValue, claimedValue - confidThreshold, claimedValue + confidThreshold)$ must return *true* for a predefined parameter $confidThreshold$. Such parameter represents the maximum allowed deviation that a testimony may have in order to determine that it supports a given $claimedValue$. At least one testimony must support such value.

Condition 3 (time consistency). All testimonies contained in *ev* must contain a time mark t_{test} such that $\mathrm{t}_{off} < \mathrm{t}_{test} < \mathrm{t}_{evid}$, being t_{off} the time of the offence and t_{evid} the time when the evidence is issued.

Condition 4 (identity consistency). Every testimony appearing in *ev* must be signed by a different entity. Moreover, there must not be a testimony created by the entity that issues the evidence header of *ev*.

Condition 5 (witness identity coherence) Every beacon contained in *ev*'s evidence header must be signed by an entity that has also issued one of the testimonies appearing in *ev*.

Confidentiality. Testimonies and evidences should only be available for EM and Adj, apart from their issuers.

Authentic requests. Only authentic requests should be processed by the receiving vehicles. A request is said to be authentic if, on the one hand, it is related to a genuine previous offence notification and, on the other, it has not been modified since it was created.

Authentic testimonies. False testimonies should be identified as such by the receiving entity. A testimony is considered to be false if the contained data is not reasonable (e.g. a vehicle may not be driven at 600 kph), if its sender is not properly identified or if it is not possible to attest that it was present (i.e. near the Requester) at the time of the facts.

7.2.3 Working assumptions

The solution devised herein is suitable to work in scenarios where the following six conditions hold. First, a secure boot-up process exists through which the CA installs all cryptography-related materials into the R and W_i's HSM. Apart from the aforementioned pseudonyms, the material contains the public-private keypairs along with the corresponding public key certificates (Cert_E(t)). Similarly, SAE applications are installed by the appropriate entity (e.g. manufacturer, road traffic agency, etc.).

The second assumption is that a Secure Location Verification (SLV) service is being executed by vehicles, to determine which vehicles are really in its vicinity [69, 70]. This avoids a vehicle falsely claiming to be somewhere, which is useful for both the Offending vehicle and the Surrounding ones. In this way, the Offending vehicle knows which vehicles are really on its vicinity and the Surrounding ones will have an accurate location for the Offending vehicle. For this purpose, vehicles verify the position of neighbours that are directly reachable by measuring the received signal strength. For those that are not reachable (for example, because of obstacles), a cooperative data exchange is performed with direct neighbours in order to discover the location of a third vehicle through triangulation.

The third assumption is related with message routing. Particularly, there exist a routing mechanism that enables sending messages from one vehicle to another. One example is the modified version of the Ad-Hoc On-demand Distance Vector (AODV), in which routes are only built for a predefined zone of relevance [71]. For the context of this work, such zone may be defined according to the maximum distance that may exist between a vehicle and its intended witnesses[1]. Additionally, a mechanism against routing misbehavior is assumed (e.g. incentive-based approach [72] or watchdog surveillance [73]).

The fourth assumption is that vehicles store the behavior-related data from all the received beacons. Such data will be removed once the next connection to the EM through the resilient channel is finished. Furthermore, it is assumed that vehicles store during a period p the information provided by in-vehicle sensors and the full set of received beacons. Such period p is assumed to be greater or equal than the time between the offence and its notification. The amount of storage required to fulfil this assumption is shown in Section 8.4.2.

The last two assumptions are related to beacons. On the one hand, it is assumed that all beacons are signed by their issuers. On the other hand, once a vehicle receives a beacon from another one, the latter will also be receiving the beacons from the former. In this way, once vehicle A receives a beacon from vehicle B, both are sure that the other one may act as its witness. Although the wireless nature of the vehicular network does not formally guarantee this situation, there are two factors that contribute on this issue. First, beacons are exchanged at a very high rate (one each 100 ms.). Second, data losses in this network do not happen in bursts, but they are independent one to each other [74]. Thus, in practice it is expected that even if A receives a beacon from B but B misses the beacon from A at the same time, the next beacon from A (which is only 100 ms. later) will be successfully received by B.

7.3 Architecture

This Section introduces the architecture derived from the model presented in Section 7.2. The considered architecture is depicted in Figure 7.3, which shows the entities from the model described in Chapter 4 (marked with a broken line) and their

[1] Such distance is related to the parameter t_{gap} that will be analyzed in Section 8.4

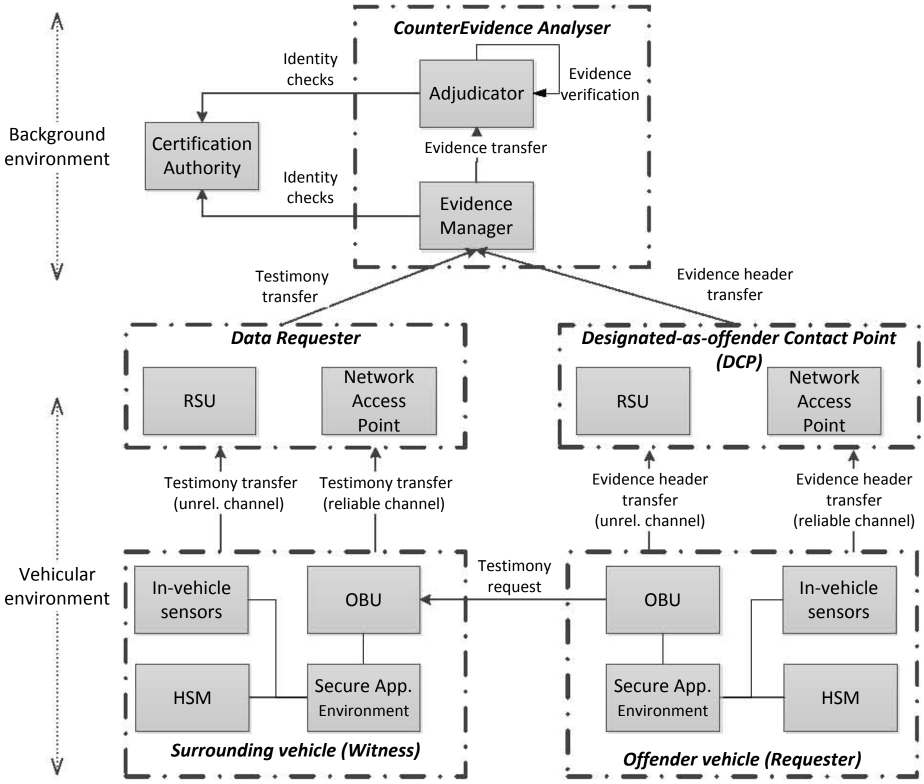


Figure 7.3: Architecture for the evidence generation protocol

technical realization. The participant entities are grouped according to the network environment they belong to, either the background or the vehicular one. Section 7.3.1 describe the background environment, whereas Section 7.3.2. Section 7.3.3 describes how both environments are connected. Section 7.3.4 focuses on the trust of entities and communication channels. The threat model is presented in Section 7.3.5. Finally, the selection of the interaction model among those presented in Section 7.2.1 is described in Section 7.3.6.

7.3.1 Background environment

There are three entities in the background environment, namely the *Certification Authority* (CA), the *Adjudicator* (Adj) and the *Evidence Manager* (EM). CA manages (i.e. issues, transfers and revokes) pseudonymous public key certificates ($\text{Cert}_{E(t)}$) that bind a cryptographic key with a pseudonym assigned to the vehicle.

Thus, CA is the top entity within a Public Key Infrastructure (PKI), and it is the only entity that is able to relate a pseudonym with a real identity [54]. Adj decides about the imposed fine taking into account the evidence proposed by the offender. Such evidence is created by EM[2], using the information received from the entities in the vehicular environment. Concerning the evidence verification and adjudication conducted by the Adjudicator, both tasks are properly within the scope of the CEA. At the light of their respective descriptions, both Adj and EM collectively form the task developed by the CounterEvidence Analyzer in the model proposed in Chapter 4. All entities that form the background environment are static, and so they are placed in one or more traditional computation nodes.

7.3.2 Vehicular environment

With respect to the vehicular environment, Requester and Witness are connected through a Vehicular Ad-hoc NETwork (VANET). For this purpose, they contain an On-Board Unit (OBU) which provides several communication interfaces (e.g. IEEE 802.11p, GPRS, etc.), as proposed in the CVIS project [75].

Apart from the OBU, there are three additional in-vehicle devices, which are organized considering the OVERSEE architecture [24]. In this way, there exists a Secure Application Environment (SAE) where applications reside. From the SAE viewpoint, the proposed protocol is an application itself.

Each vehicle is also equipped with sensors, which give information related to the vehicle current status (position, speed) and to its surroundings. All these data will be stored in a data set (Know$_E$(t)), which contains the information known by vehicle E at time t. This set is also present in the entities in the background environment to store the data received from others.

The OVERSEE architecture also considers the existence of a Hardware Security Module (HSM). Regarding this contribution, such device provides with a reliable time source and stores the cryptographic material related to vehicular credentials.

[2] Other alternatives are analysed in Section 7.3.6.

Particularly, it stores a set of short-lived pseudonyms that will be given to each vehicle to protect their privacy. They are noted as R(t) (Requester pseudonyms) and $\mathrm{W}_i(\mathrm{t})$ (Witness pseudonyms), and may be used only in time t. To avoid routing problems due to the pseudonym change, each OBU will be able to receive packets that are sent to one of its previous but recent pseudonyms [65].

7.3.3 Connection between environments

The connection between both the background and the vehicular environment may be performed through Road Side Units (RSUs)[3], which are static nodes placed aside the roads that participate in the VANET. Thus, the RSU task involves receiving some data from the offending vehicle (as it is done, in the enforcement model proposed in Chapter 4, by the Designated-as-offender Contact Point, DCP) and from witness vehicles (as it is done in the enforcement model by the Data Requester, DR).

All RSUs are connected to EM. Apart from this connection, there exists a resilient channel between the vehicular entities and the EM, which ensures that packets eventually arrive. One typical environment for such a channel is a location-restricted connection like an at-home network. This channel is built periodically, for example at a daily basis. The Network Access Point (NetAP) is the entity that enables such communication between OBUs and EM.

7.3.4 Trust model

Trust considerations are divided into those affecting entities and those for communication networks. Regarding entities, Adj is *honest-but-curious*, which means that it will never misbehave but it may try to deduct as much information as possible regarding the offender. On the other hand, both the CA and the EM are trusted. In the first case, it means that it will responsibly manage the vehicular credentials and that it will never disclose to unauthorized entities the identity related to a given

[3] Although other settings could be possible (e.g. using cellular connections), the use of RSU has been chosen for consistency with the rest of this thesis' contributions

pseudonym. With respect to the EM, it will never disclose any received information to unauthorized parties and it will never create false information, forge or manipulate any existing one. Furthermore, they will unavoidably follow the proposed protocol.

With respect to the vehicular environment, there are two fully trusted entities (HSM and SAE) and two unreliable ones (in-vehicle sensors and OBU). In the last case, it is assumed that both may be maliciously altered, thus leading to false sensorial information (in-vehicle sensors), a communication blockage or data manipulation (OBU).

Communication networks present different trust profiles. The network in the background environment is assumed to be resilient (i.e. packets eventually arrive). However, it does not prevent from manipulation, injection or eavesdropping attacks. On the other hand, the in-vehicle network between OBU, HSM and SAE is managed by the OVERSEE architecture, thus guaranteeing that only authorized parties may access and no data alteration is possible. The connection with sensors is assumed to be resilient but unreliable (i.e. there is no guarantee on the data authenticity). The same profile is shared by the resilient connection between vehicles and EM. Finally, the regular communication between vehicles, and from these to the background environment, is not resilient nor reliable.

7.3.5 Threat model

Threats on correctness. There are two threats on this issue. First, every message sent through an unreliable network (as it is the case of the vehicular one) may be altered or lost. Second, the aforementioned messages may be never created, even if mandated by the protocol. One example of this is that OBUs may be compromised in such a way that they refuse to participate in the protocol.

Threats on confidentiality. The eavesdropping threat may happen in the vehicular environment (as usual in shared medium networks such as VANETs) as well as in the background network (due to its unreliability).

Threats on authentic requests. A rational attacker may ask for testimonies referred to other vehicle as a means of obtaining some information about its past behavior.

Threats on authentic testimonies. A false testimony is not beneficial for a well-behaving vehicle, as it may lead to legal consequences. However, a rational attacker may be interested in creating testimonies without being in the surroundings of the offender, if a reward is given by the offender. Apart from this threat, a malfunctioning sensor may originate inaccurate testimonies.

7.3.6 Selection of the interaction model

Taking into account the interaction models identified in Section 7.2.1, in this Section they are comparative analysed. Furthermore, the most suitable one is selected.

Without entering into the details of the exchanged messages for each particular setting, some conclusions may be reached from the general features of each approach. Such features are the system scalability, its auditability and its effectiveness (see Table 7.2).

Regarding the system scalability, it must be noted that the decentralized choice is more scalable than the remaining approaches, as the workload from EM is reduced. Even considering that EM's computational power greatly overcomes that offered by vehicles, the amount of offences that may be detected (at a nation-wide scale) at the same time suggests that EM may become a bottleneck. However, the feasibility of this approach should be analysed, as several real-time ITS services will be running at the same time over the (constrained) vehicular computational device. On the other hand, the combined approach seems to appropriately balance the requirements from both parts. However, experimental evaluations with real vehicular hardware will be interesting to assess this issue.

The system auditability measures whether it is possible to reliably determine the operations that have been performed to achieve a result. In this context this is a critical feature, as there could be consequences after the execution of this mechanism, e.g. call for maintenance due to the lack of response by a witness. In this regard, the decentralized approach is less suitable than the remaining options. As all the inter-vehicle communications are performed over an unreliable channel, it would be impossible to determine whether the absence of a testimony (needed by a certain R) is due to the loss of the request, of the testimony or the uncooperative behaviour from W_i [66]. However, a lazy R could claim that it sent a request but did not receive a testimony, thus forcing EM to collect it. In this way, R could save resources, but it could never be determined whether its claim was trustworthy. The centralized variant is similar to the combined approach in this issue, as in both cases EM (which is trusted) takes part in the process, using the resilient channel.

The system effectiveness measures the capacity of the system to create evidences based on testimonies. The decentralized approach is again inappropriate for this context. To understand this issue, it is important to note that a testimony that is not beneficial for R could cause it to take reprisals against W_i. Moreover, it is reasonable to assume that if R would know the value of the testimonies, it will remove the ones that are not favourable to it to avoid wasting resources by creating evidences that are against its interests. In this way, a W_i holding a non-profitable value for R would never answer in the decentralized choice. Therefore, such approach would prevent these testimonies to be managed. On the contrary, the system effectiveness offered by the centralized version and the combined one is similar, as both enable a private communication between the EM and every W_i. Thus, these unfavourable testimonies could be freely sent to EM. They could be used to enable the Authority to complement its proof against the offender. For this reason, we consider that the effectiveness of the combined approach (and, similarly, of the centralized version) is better than the decentralized one.

At the light of these considerations, the combined approach is the most suitable

	Centralized	Decentralized	**Combined (selected)**
System scalability	–	++	+
System auditability	++	–	++
System effectiveness	+	– –	+

Table 7.2: Analysis of approaches for the testimony collection and evidence generation. The rating for each feature ranges from ++ (totally fulfilled) to – – (poorly fulfilled)

one as it addresses successfully all the analysed features. For this reason, it will be selected for the development of this contribution.

7.4 Protocol specification

The proposed protocol is composed by three parts, namely the testimony collection, the evidence generation and the evidence verification. Furthermore, there are two exceptional situations that must be properly handled, one concerning the offender and the other related to witnesses. The following subsections describe, first, the data structures (Section 7.4.1) and cryptographic operations at stake (Section 7.4.2) and, afterwards, each of the aforementioned process parts and the exceptional processes.

7.4.1 Data structures

There are five data structures in this work, namely beacon, testimony, request, evidence header and evidence. Beacons (noted as $\mathrm{Beacon}_S(\mathrm{t})$) contain the description of several behavior-describing variables (such as heading, acceleration, etc.) of the sender vehicle S at time t. In this work, they contain at least the speed and position, and are digitally signed to avoid manipulation. The corresponding public key certificates are sent along beacons to enable their verification. A testimony Testim_{E1} allows one vehicle E_1 to describe one of these variables related to another vehicle E_2 at a given time t_{test}. The testimony is to be used in the context of an offence notification identified by *offence-id*. To ensure the data origin, it is digitally signed by its issuer.

In order to retrieve a testimony, the Requester sends a request $\text{Req}_{R(Treq)}$, which contains the moment to which the testimony should be referred (t_{off}), the sender's identity on that moment (pseudonym $\text{R}(\text{t}_{off})$), the offence identifier *offence-id* and the behavior-describing variable that should be witnessed (i.e. position or speed). In order to prevent a third party to impersonate the Requester, the request is divided into two parts, each one signed under a different identity. Thus, the first part (called *part 1*) contains $\text{R}(\text{t}_{off})$ and t_{off} and is signed using the private key related to pseudonym $\text{R}(\text{t}_{req})$, which is the sender's identity when the request is created. In this way, both identities get linked. The second part (*part 2*) contains *offence-id* and the type of testimony requested, and it is signed under $\text{R}(\text{t}_{off})$. In this way, only the vehicle that actually holds both private keys is able to build this message.

Finally, the most complex data structure is the evidence (Evid). It is formed by an evidence header, a set of supporting testimonies and the time t_{evid}. The header $\text{EvidHdr}_{R(Tevid)}$ describes the identity of the Requester in the moment of the evidence ($\text{R}(\text{t}_{evid})$) and contains: (1) its claim on its past behavior (called *claimedValue*), (2) the identification of the offence *offence-id*, (3) the beacons that show that witnesses were in the Requester's surroundings at t_{off} (plus their corresponding public key certificates), and (4) the time marks t_{off} and t_{evHdr}. The corresponding public key certificates are also introduced to enable the verification of such beacons. The evidence header is signed by the Requester to ensure the data origin authentication. On the other hand, the whole evidence is signed by the Evidence Manager to ensure that only evidences controlled by this entity are considered by the Adjudicator.

7.4.2 Cryptographic operations and auxiliary functions

In the context of this process, public key cryptography is considered. Particularly, to protect the confidentiality of messages, public key encryption ($\text{E}_{X(t)}(\text{M})$) and its corresponding decryption ($E^{-1}_{X(t)}$(M)) will be applied. On the other hand, to ensure their integrity and data origin authentication, digital signatures ($S_{X(t)}$(M)) and their verifications ($S^{-1}_{X(t)}$(M)) are in use.

Apart from cryptographic operations, entities are able to execute seven operations related to the management of the knowledge set Know$_E$(t) and the processing of incoming messages. Within the knowledge set, vehicles may look for behaviour-related data from other vehicles through the *lookupBehRecord* function. They may also search the public key certificate of other entity using the *lookupCert* function. To find suitable witnesses for a given vehicle, it may execute the $findNeighbours$ operation. This operation relies on the Secure Location Verification service. For each one, it returns the beacon that shows that it was near that vehicle, along with the public key certificate for verifying it. Once a testimony is created, the receiving entity can store it in its knowledge set using the *storeTestimony* operation, and it may be retrieved later on using *retrieveTestimony*. In order to ensure if a claim is supported by a set of testimonies, *contains* enables to find whether a given value is within an interval (for speeds) or region (for positions).

As opposed to the previous operations, which may be executed by all entities, there is an operation (*checkPseudonymsEntity*) that is only available for the CA. Such operation enables to determine whether two different pseudonyms belong to the same entity.

7.4.3 Testimony collection

Once a vehicle has received a fine notification, its SAE determines whether it is suitable to ask for evidences to challenge the fine. In such a case, the testimony collection process is started (see Algorithm 7). For this purpose, SAE extracts the relevant information from the offence notification to build the request, namely the offence identifier and the time of the offence. Furthermore, it determines which behavior-related variable should be witnessed, and sends all these data to the HSM to build the request (Algorithm 7, lines 2,3). In order to determine the vehicles that are candidate to be witnesses, the function $findNeighbours$ is used to establish which vehicles were around the Requester in the moment of the offence (t_{off}) (line 4). For each of these vehicles, the request is sent (line 6). Apart from being signed (as explained in Section 7.4.1), the request is encrypted as it contains a private statement – the Requester, which is currently using pseudonym $\mathrm{R}(\mathrm{t}_{req})$, was using pseudonym $\mathrm{R}(\mathrm{t}_{off})$ at the time of the offence. For the same reason, the public key certificate $\mathrm{Cert}_R(\mathrm{t}_{off})$ is also encrypted. It must be noted that the Requester is able to encrypt data for witnesses as it stores, for some time interval, their public key certificates (recall Section 7.2.3).

Once a Witness W_i receives and decrypts the testimony request, it verifies the signature (line 7). Such verification includes checking the status of the requester certificates, which is important to avoid creating testimonies for a vehicle which is in an irregular situation. If such verification is correct, it searches within its knowledge any data that is relevant to R in t_{off} (line 9). If it exists, a testimony is prepared and sent encrypted to EM (lines 11-13). The encryption is necessary to avoid third parties to be aware of the witnessed value. Significantly, R should not realize of this value to avoid retaliation against W_i in case that the testimony is against R's interests. However, the public key certificate necessary to verify the signature is not encrypted, as it only contains public information. All these data are stored by EM (line 14) and will be used to create the evidence afterwards.

7.4.4 Evidence generation

When R (specifically, its SAE) estimates that all witnesses have had enough time to send their testimonies, it starts the creation of the evidence header (Algorithm 8). For this purpose, it sends to HSM_R the offence identifier, the time of the offence, the set of designated witnesses (including the beacons and the corresponding public key certificates) and its estimation (claimedValue) on the behavior-describing variable

```
Data: offence-id, the offence identifier; type, the type of evidence that
      should be created based on the type of offence purportedly
      committed; $t_{off}$, time of the offence; $t_{req}$, time in which the request is
      prepared; $t_{test}$ the time in which the testimony is created;
begin
    $SAE_R \rightarrow HSM_R$ : offence-id, type, $t_{off}$
    $HSM_R \rightarrow SAE_R$ : $Req_{R(Treq)}$
    $SAE_R$ : {neighbourSet, beaconSet, certSet} = findNeighbours(R,$t_{off}$)
    forall the $W_i \in$ neighbourSet do
        $SAE_R \rightarrow OBU_R \rightarrow OBU_{Wi} \rightarrow SAE_{Wi} \rightarrow HSM_{Wi}$ :
        $E_{Wi(Toff)}(Req_{R(Treq)}, Cert_R(t_{off})), Cert_R(t_{req})$
        $HSM_{Wi}$ : { part1, part2 } = $E^{-1}_{Wi(Toff)}(Req_{R(Treq)}, Cert_R(t_{off}))$
        if $S^{-1}_{R(Treq)}$(part1) = true & $S^{-1}_{R(Toff)}$(part2)=true then
            $HSM_{Wi} \rightarrow SAE_{Wi}$ : RequestedFact =
            lookupBehRecord($Know_{Wi}(t_{off})$, $R(t_{off})$,$t_{off}$, type)
            if RequestedFact is not null then
                $SAE_{Wi} \rightarrow HSM_{Wi}$ : RequestedFact, EM
                $HSM_{Wi}$ : lookupCert($Know_{Wi}(t_{test})$, EM, $t_{test}$)
                $HSM_{Wi} \rightarrow OBU_{Wi} \rightarrow$ RSU $\rightarrow$ EM: $E_{EM}(Testim_{Wi(Ttest)})$,
                $Cert_{Wi}(t_{test})$
                EM : storeTestimony(EM, $E^{-1}_{EM}(Testim_{Wi(Ttest)})$,
                $Cert_{Wi}(t_{test})$)
```

Algorithm 7: Testimony collection

(line 2). Such header is then sent to EM through one RSU (line 3) encrypted to prevent other vehicles to learn the status data of witnesses. Again, the public key certificate is not encrypted as it is not confidential. EM then decrypts and verifies the evidence header signature. If it is not correctly signed, the evidence header is discarded. Otherwise, EM acknowledges such header (lines 4-7). It must be noted that if the acknowledgement is not received within a reasonable time interval (considering the EM processing speed and the transmission delays), R starts the corresponding Exception Handling procedure (see Section 7.4.6). This situation may happen because one of four reasons: the evidence header was lost, it was not correctly signed, the acknowledgement was lost or not correctly signed.

If the evidence header was correctly received and verified, EM compiles the evidence incorporating the corresponding testimonies based on the witness list provided in such evidence header (lines 9-14). If any of them has not been received, the Testimony Exception Handling procedure is marked to be started once the witness connects using the reliable channel (see Section 7.4.6). Once all the available testimonies have been collected, the evidence is finished. EM transfers it to Adj (line 15), which will verify it as a prerequisite to the adjudication process.

Taking into account the described procedure, the need for R to wait an interval to promote all witnesses to have sent their testimonies is based on how exceptions are managed. Particularly, the absence of one Testimony causes the initiation of the Testimony Exception Handling. As this process requires the reliable channel, it introduces a non-negligible delay in the whole evidence generation process. Thus, the waiting time for R tries to maximize the chance for testimonies to have been sent to EM whenever they are required, avoiding the use of the exception handling procedure. The estimation of this waiting time should be based on the computational capabilities of vehicles and the inherent transmission delays for the testimony.

```
Data: offence-id, $t_{off}$, beaconSet, neighbourSet, certSet, from Algorithm 7;
      claimedValue, SAE estimation on the behavior-describing variable;
begin
    $SAE_R \rightarrow HSM_R$ : offence-id, claimedValue, $t_{off}$, beaconSet, certSet
    $HSM_R \rightarrow SAE_R \rightarrow OBU_R \rightarrow RSU \rightarrow EM : E_{EM}(EvidHdr_{R(Tevid)})$,
    $Cert_R(t_{evid})$
    EM : decryptedHeader = $E^{-1}_{EM}(EvidHdr_{R(Tevid)})$
    EM : result = $S^{-1}_{R(Tevid)}$(decryptedHeader)
    if result = true then
        $EM \rightarrow RSU \rightarrow OBU_R \rightarrow SAE_R \rightarrow HSM_R : S_{EM}(ACK_{evHdr}$,
        offence-id)
        # If the acknowledgement is not received, or not successfully verified,
        the evidence header exception handling is invoked (Algorithm 11)
        EM : SupportingTestim = null
        # neighbourSet is composed by the identifiers of senders of beacons
        in beaconSet
        forall the $W_i \in neighbourSet$ do
            EM : CurrentTestimony = retrieveTestimony($Know_{EM}(t_{evid})$, $W_i$,
            offence-id, $t_{off}$)
            if CurrentTestimony = null then
                EM : call Testimony exception handling algorithm (Algorithm
                10) and store the result in CurrentTestimony
            EM : SupportingTestim = SupportingTestim $\cup$ CurrentTestimony
        $EM \rightarrow Adj : E_{Adj}(S_{EM}(Evid_{EM}))$
```

Algorithm 8: Evidence generation

Dealing with witnesses that have invalid certificates

Under some circumstances, vehicles may have their certificates invalid. This may happen, for example, if a vehicle has misbehaved, or if it has not accomplished the underlying administrative processes (e.g. yearly inspections, tax renewal, etc.).

In this context, the testimony provided by a vehicle in this irregular situation is not valid, as it will not be correctly signed. From the requester point of view, there are two potential approaches that may be used to deal with these vehicles – the *a priori* approach and the *a posteriori* one. In the *a priori* approach, the requester has already verified the incoming beacons, and therefore it determines that the sender is not a suitable testimony. Therefore, it does not issue a request for this vehicle and, consequently, it does not take part in this process. In the *a posteriori* approach, the requester first sends the request to that vehicle and, afterwards, it verifies the beacons that showed that the witness was in the requester's surroundings. In case that it finds that the certificate status was invalid, then the witness is not included in the witness list within the evidence header. According to the evidence generation process, at the end the testimony potentially provided by such a vehicle would not be considered.

From the sake of efficiency, the a priori approach is more interesting, as it avoids creating and sending an unnecessary request. Nevertheless, it must be noted that it requires that the verification is performed beforehand. As in both cases the testimonies from vehicles holding an invalid certificate will not be considered, the decision depends on the availability of resources to perform such computation at the required time.

7.4.5 Evidence verification

The evidence verification process (Algorithm 9) is executed mainly by Adj and starts by verifying the signatures on the evidence and on each of the beacons contained in the evidence header (lines 2-7). It should be noted that the signature on the evidence header was already verified by EM during the evidence generation. If any of these verifications fail, the whole evidence is discarded, as it is conceptually invalid. This also applies in case that it is one beacon which is not successfully verified. It should be noted that the vehicle should have already verified such beacon, so an invalid signature indicates that the vehicular devices are not operating regularly.

In case that all the aforementioned verifications are successful, the checks on the content may start. First, it is evaluated if the verification is performed in a moment later than that in which the evidence was created (line 8). In such a case, each of the testimonies is analysed. If its signature is verified (line 11), then several checks are applied over the contents of the evidence – coherence of times, of identities and of the behavior-describing values. Thus, the testimony must be created at a reasonable time (i.e. after the fine notification but before the evidence time) (line 12). It should be noted that there is no need to verify if the testimony is issued by one of the witnesses designated by R, as EM only considers witnesses included in *neighbourSet* in the evidence generation. However, all participants (i.e. R and all W_is) must be different among them. To this regard, Adj contacts the CA in order to ensure that the different pseudonyms are not related to the same entity (lines 13-17). In case that an identity fraud is detected, the verification process is aborted and the CA is contacted to reveal the identity of the involved entity. Similarly, Adj takes the same decision if R is not related to the offence identified by $offence-id$[4].

If all the previous inspections are successful, it is evaluated whether the witnessed value supports R's claim, i.e. belongs to a confidence interval around $claimedValue$, using a predefined confidence parameter $confid-threshold$ (lines 18-20). If it is the case, the index that counts the amount of supporting testimonies (*supportIndex*) is incremented.

The process is repeated for all the beacons that were contained in the evidence header. The result of this process is twofold. First, the boolean value $verified$

[4] It should be noted that issuing a request, validly signed, related to an offence in which the requester is not involved, is an irrational behavior which does not report any valuable benefit.

which indicates if the evidence header signature was successfully verified. Second, the final result of *supportIndex* shows the degree of support that the requester claim has. Such value may be useful for a posterior adjudication process. It should be noted that if there is no supporting testimony, the evidence is considered as not semantically valid. This fact is reflected by putting $verified$ to false (lines 20-22).

7.4.6 Exception handling

There are two exceptional situations, caused by the data loss in the communication channel. The first one is the absence of an expected testimony, which may happen if the witness did not receive the request, the testimony itself was lost or even the purported witness did not know the requesting vehicle. The second one is the lack of acknowledgement for the evidence header, which makes the Requester be unaware of the successful starting of the evidence generation by the EM. This may be caused because either the evidence header or its acknowledgement were lost in transmission. Each situation must be managed using a different exception procedure. In order to avoid the uncertainty caused by the channel unreliability, these exception handling mechanisms are run over the resilient channel between the vehicular entities and EM.

Testimony exception handling

Once the resilient channel is established, there exist a mutual authentication process between EM and the connected vehicle. As this process is executed at time t_{exc}, the vehicle will be using the pseudonym $\mathrm{W}_i(\mathrm{t}_{exc})$. After this authentication, EM determines whether the connected vehicle was supposed to give one testimony that has not been received yet. For this purpose, it uses the function *checkPseudonymsEntity* from the CA, considering the list of all witnesses that have a pending testimony to send. If it is the case, the testimony exception handling is invoked (Algorithm 10). EM asks for a testimony by sending the offence-related

```
Data: Evid$_{EM}$, the evidence at stake; t$_{verif}$ time in which the evidence is
      verified; confid-threshold, the maximum allowed deviation over the
      claimed value in order to consider that it is supported by another
      claim; t$_{evid}$, the time when the evidence is created; testimonyValue,
      the value reported by the witness
Result: verified: true if the evidence is correct, false otherwise;
        supportIndex: amount of testimonies supporting the claim
begin
    Adj : resultEvid = $S^{-1}_{EM}(Evid_{EM})$
    Adj : resultBeacon = true
    forall the $Beacon_{Wi(Toff)}$ in $EvidHdr_{R(Tevid)}$ do
        Adj : resultBeacon = $S^{-1}_{Wi(Toff)}(Beacon_{Wi(Toff)})$
        if resultBeacon = false then
            break
    if resultEvid = true & resultBeacon = true & $t_{verif} > t_{evid}$ then
        Adj : verified = true
        forall the $Testim_{Wi(Ttest)}$ in SupportingTestim in $Evid_{EM}$ do
            Adj : resultTestim = $S^{-1}_{Wi(Ttest)}(Testim_{Wi(Ttest)})$
            if resultTestim = true & $t_{evid} > t_{test} > t_{off}$ then
                Adj → CA : $W_i(t_{test})$ [from the certificate], $R(t_{off})$ [from the
                testimony]
                CA → Adj : cheatingReq =
                checkPseudonymsEntity($W_i(t_{test})$,$R(t_{off})$)
                # Checking that all witnesses are different one to each other,
                and that the R is related to the offence at stake, is omitted for
                brevity
                if cheatingReq = $false$ then
                    Adj: supportEvaluation = contains(testimonyValue,
                    $claimedValue - confid - threshold/2$,
                    $claimedValue + confid - threshold/2$)
                    if supportEvaluation = true then
                        Adj : supportIndex = supportIndex+1
                else  # Detected identity fraud, abort process and proceed
                with identity reveal
        if supportIndex = 0 then
            verified = false
    else  verified ← false ; supportIndex ← 0
    return verified, supportIndex
```

Algorithm 9: Evidence verification

data: which offence is related (*offence-id*), who was involved (R(t_{off})) and when it happened (t_{off}). Moreover, it also sends the beacon that shows that the asked vehicle may potentially act as a witness of the offence (line 2). The whole message is encrypted to prevent eavesdropping, except the public key certificate of EM which is not private. It should be noted that the data sent by EM reveals W_i's past location (contained in the beacon) and such data should be kept private. W_i then decrypts and verifies the enquiry (line 3-4) and proceeds to prepare the testimony. The first action is to determine if the purported witness has any relevant data to build the testimony (line 5). In such a case, it is built and sent encrypted to EM (lines 6-8). The testimony should be kept private to avoid R be aware of its contents. It must be noted that the probability of R being aware of this transmission is extremely low – it should be in the coverage area of the place where W_i establishes this resilient channel with EM. However, the potential undesired consequences of not encrypting such information are bigger than the cost of the encryption operation.

In case that the witness does not have the information to build the testimony, the vehicle answers indicating this issue (lines 15-17). This is a signed message which contains an indication of this issue ($f_{not-ready}$) and the offence identifier. It is not encrypted as none of these data are private by themselves.

Based on the answer, EM takes different actions. If the testimony is received and correctly verified, then it is transferred to the evidence generation process to insert it into the ongoing evidence (lines 8-15). On the other hand, if the signature on the vehicle claim for not being a witness is also correct, EM continues with the evidence generation omitting this vehicle as a witness (lines 19-20). However, the Authority may implement a mechanism to avoid a malicious use of such action, which should be exceptional – it has been assumed that beacons are mutually exchanged. Finally, if the signature is not correct or there is no answer from the vehicle, then the vehicle is called for maintenance to verify the vehicular devices (lines 11, 19).

```
Data: EvidHdr$_{R(Treq)}$, the evidence header; t$_{exc}$ current time, Cert$_{Wi}$(t$_{test}$)
      the certificate of the witness
begin
    EM → NetAP → OBU$_{Wi}$ → SAE$_{Wi}$ → HSM$_{Wi}$ : enquiry =
    E$_{Wi(Texc)}$(S$_{EM}$(Beacon$_{Wi}$(t$_{beacon}$), R(t$_{off}$), t$_{off}$, offence-id, type),
    Cert$_{EM}$(t$_{exc}$)
    HSM$_{Wi}$ → SAE$_{Wi}$ : result = S$^{-1}_{EM}$(E$^{-1}_{Wi(Texc)}$(enquiry))
    if result = true then
        HSM$_{Wi}$ → SAE$_{Wi}$ : RequestedFact =
        lookupBehRecord(Know$_{Wi}$(t$_{off}$), R(t$_{off}$),t$_{off}$, type)
        if RequestedFact is not null then
            SAE$_{Wi}$ → HSM$_{Wi}$ : RequestedFact, Cert$_{EM}$(t$_{exc}$))
            HSM$_{Wi}$ → OBU$_{Wi}$ → NetAP → EM: E$_{EM}$(Testim$_{Wi(Ttest)}$),
            Cert$_{Wi}$(t$_{test}$)
            EM: result = S$^{-1}_{Wi(Ttest)}$(E$^{-1}_{EM}$(Testim$_{Wi(Ttest)}$))
            if result = $false$ then
                EM : Call vehicle for maintenance
            else
                EM : Continue with Evidence Generation (Algorithm 8) using
                this testimony
        else
            SAE$_{Wi}$ → HSM$_{Wi}$ : f$_{not-ready}$, Cert$_{EM}$(t$_{exc}$))
            HSM$_{Wi}$ → OBU$_{Wi}$ → NetAP → EM : claimNotReady =
            S$_{Wi(Texc)}$(f$_{not-ready}$, offence-id)
            EM : result = S$^{-1}_{Wi(Texc)}$(claimNotReady)
            if result = $false$ then
                EM : Call vehicle for maintenance
            else
                EM : Continue with Evidence Generation (Algorithm 8)
                omitting this testimony
```

Algorithm 10: Testimony Exception handling

Evidence header exception handling

This process is activated if SAE$_R$ does not receive the acknowledgement for the evidence header (Algorithm 11). As opposed to the transference of testimonies, the evidence header requires an acknowledgement to enable R be aware of the starting of the evidence generation process. In this process, R sends the evidence header (line 2), which was already created and encrypted for EM in the evidence generation part. If the signature on the evidence header is not successfully verified, the vehicle is called for maintenance as a preventive measure (lines 3-7). Otherwise, an acknowledgement is issued in the same way as it was done in the evidence generation (line 8). As the acknowledgement is signed to ensure its integrity and data authentication, it may happen that the signature verification (lines 12-13) fails. In such a case, this process is restarted. In this way, this process only finishes when the acknowledgement is successfully received by R.

```
Data: $E_{EM}(\text{EvidHdr}_{R(Tevid)})$, encrypted evidence header already created in
      the evidence generation process
1  begin
2      $\text{SAE}_R \rightarrow \text{OBU}_R \rightarrow \text{NetAP} \rightarrow \text{EM} : E_{EM}(\text{EvidHdr}_{R(Tevid)}), \text{Cert}_R(t_{evid})$
3      EM : decryptedHeader = $E^{-1}_{EM}(\text{EvidHdr}_{R(Tevid)})$
4      EM : result = $S^{-1}_{R(Tevid)}$(decryptedHeader)
5      if $result = false$ then
6          EM : Call for maintenance
7      else
8          $\text{EM} \rightarrow \text{NetAP} \rightarrow \text{OBU}_R \rightarrow \text{SAE}_R \rightarrow \text{HSM}_R$: acknowledgement =
           $S_{EM}(\text{ACK}_{evHdr}$, offence-id)
9          if $EvidHdr_{R(Tevid)}$ had not been previously received then
10             EM : Proceed with the Evidence generation process (Algorithm
               8), from line 9
11         $\text{HSM}_R \rightarrow \text{SAE}_R$ : result-ack = $S^{-1}_{EM}$(acknowledgement)
12         if $result\text{-}ack = false$ then
13             $\text{SAE}_R$ : restart evidence header exception handling process
```

Algorithm 11: Evidence header exception handling

It should be noted that this process may be run by R simply because the acknowledgement, but not the evidence header itself, was lost. In such a case, EM would have already performed the steps of the Evidence generation algorithm that are beyond the acknowledgement. Otherwise (lines 9-11) it is necessary for EM to proceed with such steps.

7.5 Summary of the chapter

In this Section a protocol for creating evidences about a vehicle's recent behavior has been presented. Data employed for creating such evidence is obtained from the neighbouring vehicles, which act as witnesses. In this way, an enriched description of the situation is achieved, thus simplifying the future decision process (e.g. liability attribution in accidents, adequate punishment for an offence). The corresponding verification process for the aforementioned evidence has also been described.

Part IV

Evaluation and Conclusions

Chapter 8

Evaluation

This Section describes the evaluation of the contributions proposed in this thesis. Thus, the enhanced model and its realization using ITS technologies is analysed in Section 8.1. The evaluation of the steganographic mechanism to send reports of misbehaving vehicles is shown in Section 8.2. The vehicular-enhanced notification protocol is analysed in Section 8.3. The mechanism for cooperative evidence generation is evaluated in Section 8.4. Finally, the novelty of the four contributions as compared to previous related works is discussed in Section 8.5.

8.1 Evaluation of the proposed enhanced enforcement model and its realization by ITS

The model proposed in this work must be suitable to represent automated enforcement systems. Although such a completely automated system does not exist, there are partially automated ones which should be represented as well by this model. In this Section this property is validated against two significant enforcement systems, the Spanish ESTRADA and the French CSA (Section 8.1.1). Additionally, the proposed application of ITS technologies in this context may produce improvements but it may also have some drawbacks. Such discussion is presented in Section 8.1.2.

8.1.1 Suitability evaluation against current systems

In order to determine the suitability of the proposed model to current systems, the entities identified in the model have been matched with the different functional parts of each system The results of such matching are summarized on Table 8.1. The granularity (i.e. level of specificity) of the matching is related to that of the functional description. Thus, the ESTRADA description enables specifying which module of the whole system is in charge of a set of operations. On the contrary, the CSA description only establishes which operations are carried in the national processing centre (referred to as CACIR, Centre Automatisé de Constatation des Infractions Routières) and those that are performed by other entities.

In general words, it may be seen that almost all functionalities of both systems have been clearly identified in the proposed model (see Table 8.1). There are two exceptions on this issue. The first one affects to the task performed by the Data requester entity, which was not explicitly detailed in any of the studied systems. The second one is related to the appealing phase, which is out of the scope of CSA. As a result, the suitability of these parts of the proposed model are not completely contrasted.

Validation against the Spanish ESTRADA

Regarding the ESTRADA, the Evidence collector is performed in two different entities of the Spanish traffic agency (called DGT) that are related to the radar and surveillance cameras management. On the other hand, the Notifier operations are performed by regular mail (managed by the Spanish postal company) or by electronic one (managed by the electronic notification module of the DGT's Data Processing Centre (DPC)). The Designated-as-offender contact point is performed in the module M2 of the ESTRADA processing centre.

With respect to the process management entities, they are placed in different modules of the ESTRADA centre except from the different fine issuance entities (Initial, Intermediate and Final fine issuers), which are placed in the Enforcement process module of the DGT's DPC.

The data management entities are placed in different modules. The Designated-

Model entity	CSA	ESTRADA
Evidence collector	Pictures received and decoded in the National Processing Centre (CACIR)	Radar management system and Picture server of the Spanish Traffic Authority
Data requester	*Not explicitly detailed*	*Not explicitly detailed*
Notifier	Regular mail sent by the national postal system (La poste)	Regular (certified) mail; Electronic mail (Electronic notification module in the Data Processing Centre of the Spanish Traffic Authority)
Designated-as-offender contact point	Regular mail to National Processing Centre	ESTRADA M2 module (Paper-based documentation received and classified)
Evidence Analyzer	Offender data retrieved by the National Processing Centre	ESTRADA M1 module (Owner data retrieval)
Initial Fine Issuer	Automated process under the supervision of the Public Prosecutor Officer	Enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
Liable Driver Analyzer	Analyzed by the National Processing Centre	ESTRADA M3 module (Citizen-given data processing)
CounterEvidence Analyzer, Allegation analyzer	The Public prosecutor analyzes the material provided by the Designated-as-offender	ESTRADA M3 module (Citizen-given data processing), although the processing of counterevidences is not explicited
Intermediate Fine Issuer	The Public prosecutor creates this fine	Enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
Process Analyzer	The case is heard by a Police court in case that the previous allegation/counterevidence has not suspended the fine	ESTRADA M3 module (Citizen-given data processing)
Final Fine Issuer	The Police court issues this final fine	Enforcement process module in the Data Processing Centre of the Spanish Traffic Authority
Appeal Analyzer	*Out of the scope of CSA*	ESTRADA M3 module (Citizen-given data processing) and Appeal and allegation system in the Data Processing Centre of the Spanish Traffic Authority
Appeal Result Issuer	*Out of the scope of CSA*	Appeal and allegation system in the Data Processing Centre of the Spanish Traffic Authority
Designated-as-offender personal data manager	National driving license database; EUCARIS	Spanish driver and offenders register; EUCARIS
Vehicle data manager	National license plate database; EUCARIS	Spanish vehicle register; EUCARIS
Process data manager	Held within the National Processing Centre	ESTRADA M2 module (Envelope removal, classification, digitalization, storage)

Table 8.1: Model suitability validation against ESTRADA and CSA

as-offender personal data manager is performed by the Spanish driver and offender register, whereas the Vehicle data manager is at the national vehicle register, both placed in the aforementioned DPC. In both cases, they may also be realized by the EUropean CAR and driver Information System (EUCARIS). Regarding the process data management, it is jointly addressed by the module M2 of the ESTRADA centre, along with the Document manager of the DPC.

Validation against the French CSA

In this system, the evidence collection and analysis are performed by the National Processing Centre (called CACIR). On the other hand, the communication to and from the offender is performed exclusively by regular post, managed by the national French postal company. The initial fine issuance is also addressed by the CACIR, although it is supervised by the Public prosecutor officer.

Beyond the starting phase, the remaining enforcement process is conducted manually. Particularly, the preliminary investigation is performed by the Public prosecutor, whereas the Process resolution is done by a police court.

Regarding the data management, both the Designated-as-offender and the Vehicle data management are performed in national databases. The use of EUCARIS has also been established as well. Finally, the Process data management entity is performed in the CACIR processing centre.

8.1.2 Analysis of the improvements and drawbacks of integrating ITS technologies in enforcement

This Section describes the improvements and drawbacks of integrating ITS-related technologies to contribute on solving the current problems of enforcement systems (recall Section 4.7). Tables 8.2, 8.3 and 8.4 summarize the comparison between current practices and the envisioned ITS-enhanced ones. Such Tables also detail the entities in the model that are affected by each approach.

Use of ITS technologies on offender identification

As opposed to cameras, ITS techniques allow the driver to be identified in a shorter time. With cameras it is the vehicle owner who identifies the real offender, and this action may take several days. Instead, ITS techniques require a few seconds or minutes depending on the availability of resources. This improvement is smaller if this identification is performed by police patrols, as it only requires the time to physically check the credentials and fill up a form. Concerning the incurred costs, deploying and maintaining the ITS infrastructure (e.g. set of Road-Side Units) requires a significant investment, which is assumed to be higher than current costs. However, extensive cost-benefit analysis have concluded the long-term suitability of ITS developments [76].

A key factor in this comparison is the global effectiveness of each approach, that is, the amount of detected offences in which the offender is reliably identified. Such effectiveness is potentially low for cameras due to identification errors or frauds. Police patrols are moderately effective, because even if they reliably identify the offender, they can only operate at specific places and times. ITS-based solutions enable a continuous reliable authentication of offenders wherever they are installed. Although there exists the chance for the driver to steal other person's credential, biometric approaches may contribute on this issue. Therefore, this approach is highly effective if deployed at a wide scale.

Use of ITS technologies to reduce notification delays

Thanks to ITS technologies, the driver may be aware of the punishment during the same trip in which the offence was committed. On this regard, they outperform traditional surveillance cameras and are similar to police enforcement. It must be noted that ITS technologies may only contribute on reducing two of the three delay factors ($t_{send.notif}$ and $t_{delay.access}$) to the order of minutes[1]. To achieve the

[1] These values are analysed in Section 8.3.1.

improvement it is also necessary to reach a negligible $t_{prep.notif}$, which requires an adequate background processing infrastructure.

The improvement on the overall speed has also an impact on the cost analysis. Thus, even if the cost of the ITS infrastructure is again significant, the process duration is reduced and therefore the cost of the bureaucracy is decreased. On the other hand, this novel notification method is more reliable than the postal one, where outdated information may cause the notification loss. Therefore, it is considered as reliable as current electronic or manual alternatives.

Use of ITS technologies to build a more complete offence description

The costs of the ITS-based improvements are again greatly higher than those required for the operation of current systems. However, they enable having data currently not available, which is a significant benefit. Moreover, such data can be available *a few seconds* after the offence, at any place where two or more vehicles coincide. This may also help victims of offenders to rapidly report them. This fact opens the door for a continuous road monitoring (as opposed to current spot-based surveillance) which promotes a permanent compliance with traffic rules. However, the same reason dictates that ITS techniques must integrate privacy protection mechanisms [54][56].

Problem	Type of system	Realization	Time taken	Cost	Reliability/Robustness	Implementing entities
Offender identification	**Current**	Vehicle keeper nominates the offending driver (postal)	$t_{send-notif}$ (postal) + 15 days	Postal parcel	False driver nomination	Vehicle owner + Designated-as-offender Contact Point
		Vehicle keeper nominates the offending driver (electronic)	$t_{send-notif}$ (electronic) + 15 days	Electronic transmission		
		Police patrols stop the offending car	Aprox. 5-10 minutes (check credentials)	Human resources, car patrol	Depends on the ability to identify persons and the chance to counterfeit documents	Police officer
	ITS-enhanced	Electronic authentication protocol between infrastructure and vehicle. Use of National e-ID cards and Electronic Driving License	Minutes (Depends on the availability of devices and network.)	Use of RSUs	Chance to use other person (e.g. co-pilot) credentials, reduced by biometry	Automatic sensor devices + Offending ITS-enabled vehicle

Table 8.2: Current enforcement systems vs. ITS-enhanced ones. Analysis on offence identification

Problem	Type of system	Realization	Time taken	Cost	Reliability/Robustness	Implementing entities
Notif. delay	**Current**	Postal notification	45 days [11]	Postal parcel	Outdated info may cause data losses	Notifier + Vehicle owner / Current driver
		Electronic notification	12 days [11]	Use of Inf. Systems	High (but subject to availability of Inf. Systems)	Notifier + Vehicle owner / Current driver
		Police patrols stop the offending car	Aprox. 15 minutes (fill up the form)	Human resources, car patrol	High / Full	Police officer
	ITS-enhanced	Electronic notification protocol directed to the offending vehicle. Use of OBU and HSM	Minutes (Depends on the availability of devices and network.)	Use of RSUs	High, as vehicles will be almost permanently connected and resilient connection is periodically available (end of journey, gas stations, etc.)	Notifier + Offending ITS-enabled vehicle

Table 8.3: Current enforcement systems vs. ITS-enhanced ones. Analysis on notification delay

Problem	Type of system	Realization	Time taken	Cost	Reliability/Robustness	Implementing entities
Offence description	**Current**	Human witnesses	Minutes	Time consumption (witness declaration)	Psychological factors, limits of perception, may affect the reliability. Lack of additional proofs	Human witness
		Cameras/radars	Immediate	Use of such devices	Automatic Number Plate Recognition has an efficiency of 90%. Weather conditions and daylight affect to their reliability	Automatic sensor device
		Policemen	Aprox. 15 minutes (fill up the form)	Human resources, car patrol	Limits of perception may affect the reliability	Police officer
	ITS-enhanced	Use of in-vehicle sensors contrasted with aggregated data electronically shared between vehicles (e.g. VANET beacons)	Seconds (Depends on the availability of devices and network.)	Use of receiving devices by the Authority (RSUs,...)	Sensorial errors are possible, but their impact may be limited, as several viewpoints (i.e. surrounding vehicles) may be available	Data Requester + Surrounding ITS-enabled vehicle

Table 8.4: Current enforcement systems vs. ITS-enhanced ones. Analysis on offence description

8.2 Evaluation of the mechanism to report misbehaving vehicles

The use of steganography to covertly report misbehaving vehicles as proposed in this work involves modifying the original data elements to embed information. If it is done over a safety-related data element (as it is the case of most sensor measurements), it is necessary to analyse the introduced error. In this Section, the ratio of altered bits is analysed (Section 8.2.1). The robustness of the system is analysed given certain configuration (parameters K and R) in Section 8.2.2. The computational and operational feasibility of the system are discussed in Sections 8.2.3 and 8.2.4 respectively. Finally, the achievement of the imposed requirements is analysed in Section 8.2.5.

8.2.1 Ratio of altered bits

By design, the maximum error introduced in each sensorial data element d_i is, at most, its accuracy $accy_{d_i}$ (see Table 5.1). From our point of view, this error is acceptable, especially considering that its effects on the road safety are minimized thanks to the embedding interval K.

In order to measure the introduced alteration, a Ratio of Altered Bits (RAB) is calculated against the total number of bits that carry sensorial information. Note, however, that this ratio does not specify the overall error introduced by our system, as different measurements are modified. The maximum number of bits altered in each beacon is given by its capacity, which is calculated in Table 5.1 and equals 24 bits. On the other hand, the total number of bits that carry sensorial information in a beacon is 224. As the proposed scheme establishes an embedding interval parameter K, the ratio of altered bits RAB is given by Equation 8.1.

$$RAB\ (Ratio\ of\ Altered\ Bits) = \frac{\sum_{i=0}^{n} capacity_{d_i}(bits)}{K \cdot \sum_{i=0}^{n} length_{d_i}(bits)} = \frac{24}{K \cdot 224} \tag{8.1}$$

Therefore, when $K = 1$, the RAB is 10.71%. Increasing the value of K reduces the RAB. That is, for $K = 2$, $RAB = 5.36\%$; for $K = 3$, $RAB = 3,57\%$; for $K = 4$, $RAB = 2.68\%$; and for $K = 8$, $RAB = 1.34\%$.

8.2.2 Robustness of the system

The communication reliability of DSRC affects the robustness of the proposed system, as there exists a non negligible probability of losing a packet that has been sent through the VANET. In this Section, the conditions (minimum number of repetitions R_{min}) under which the system is robust (to a certain probability $p_{threshold}$) are studied.

Let p_{beacon} and p_{msg} be the probability of successful reception of a beacon and an embedded message, respectively. If the reception of each beacon is considered an independent event, p_{msg} can be calculated as a function of nb_{msg} and p_{beacon} as follows:

$$p_{msg} = (p_{beacon})^{nb_{msg}} \tag{8.2}$$

The success probability $p_{success}$ is defined as the probability of that at least one of the R repetitions has successfully reached the receiver. Thus, $p_{success}$ can be calculated using the aforementioned p_{msg}:

$$p_{success} = 1 - (1 - p_{msg})^R \tag{8.3}$$

To ensure the system robustness, $p_{success} > p_{threshold}$ must hold under all configurations of the system. Such condition imposes the minimum number of repetitions $R_{min}(p_{threshold})$, which is graphically shown in Figure 8.1. For this calculation, p_{beacon} is assumed to be 0.58, which is the value estimated in [74] for the packet delivery ratio in VANETs for packets sent from a distance of 400 meters (vehicle-to-vehicle). Note that Figure 8.1 shows not only R_{min} for $nb_{msg} = 9$ (the case of the proposed system) but also for $nb_{msg} = 11$ and $nb_{msg} = 7$, so the effects of increasing

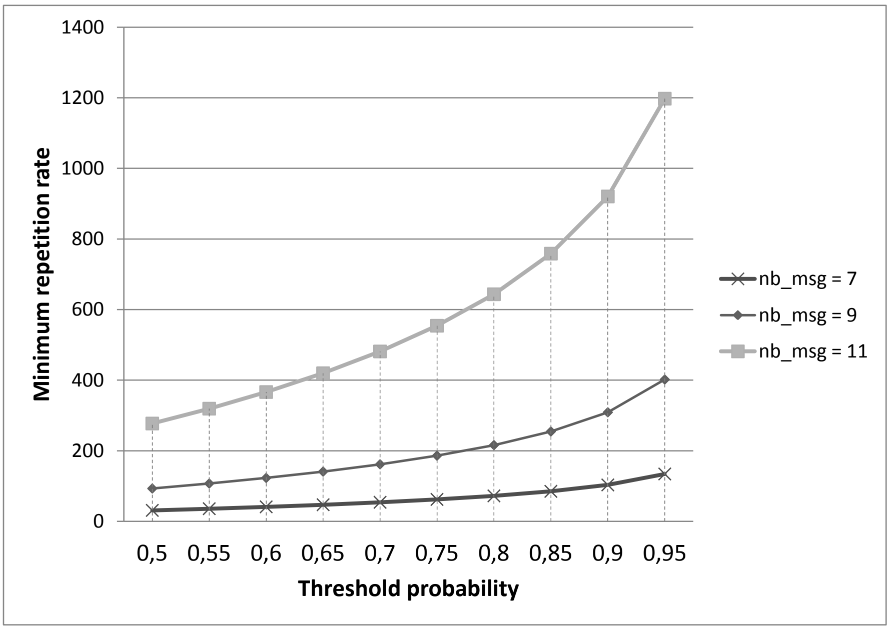


Figure 8.1: Analysis of the minimum repetition rate R_{min} once a threshold probability $p_{threshold}$ is selected. It is assumed that $p_{beacon} = 0.58$. In the proposed system $nb_{msg} = 9$.

or decreasing the number of fragments nb_{msg} are illustrated.

8.2.3 Computational feasibility

In this Section it is analyzed if all participants in the system are computationally capable of sending and receiving hidden messages. The time required by the sender and receiver is reflected in Equations 8.4 and 8.5, respectively. It must be noted that they reflect the cost considering the whole set of R repetitions (although it is highly improbable that the RSUs will successfully receive all of them).

$$\begin{aligned} T_{SND} &= T_{prepare} + R \cdot T_{embedding} = T_{prepare} + R \cdot (T_{protect} + T_{substitute}) = \\ &= T_{prepare} + R \cdot (T_{ECIES-keys} + T_{ECIES-encrypt} + T_{ECIES-MAC} + \\ &+ nb_{msg} \cdot T_{substitute-beacon}) \end{aligned} \tag{8.4}$$

$$\begin{aligned} T_{RCV} &= R \cdot (T_{detect} + (nb_{msg} - 1) \cdot T_{finish\text{-}revealing}) = \\ &= R \cdot (nb_{msg} \cdot T_{extract\text{-}beacon} + T_{ECIES\text{-}keys} + T_{ECIES\text{-}encrypt^{-1}} + \\ &+ T_{ECIES\text{-}MAC^{-1}} + T_{reassemble}) \end{aligned} \tag{8.5}$$

For each report, the sender first prepares the secret message ($T_{prepare}(56\ bits)$). Afterwards, for each repetition R, he derives the keys ($T_{ECIES\text{-}keys}$), protects the secret message ($T_{ECIES\text{-}encrypt}(56\ bits)$ and $T_{ECIES\text{-}MAC}(56\ bits)$) and embeds the fragments in each of the nb_{msg} beacons that follow ($T_{substitute\text{-}beacon}(216\ bits)$).

With respect to the receiver, the first part of its effort (T_{detect}) is devoted to decide whether there is an embedded secret or not in a given beacon. This operation may be further divided into the time to extract the bits ($T_{extract}(24\ bits)$), the time to derive the keys ($T_{ECIES\text{-}keys}$) and the time to decrypt the extracted bits ($T_{ECIES\text{-}decrypt^{-1}}(24\ bits)$). It is important to note that this effort will likely happen for every received VANET message whose identifier complies with the defined embedding interval K, until the existence of a secret message is confirmed.

Once the RSU detects that it is receiving an embedded message from certain vehicle (T_{detect}), its revealing must be finished ($T_{finish\text{-}revealing}$). There will be $nb_{msg} - 1$ more fragments to process, involving the time to extract the bits ($T_{extract\text{-}beacon}(192\ bits)$), the time to decrypt them ($T_{ECIES\text{-}encrypt^{-1}}(32\ bits)$) and to verify the MAC value on the whole set of bits ($T_{ECIES\text{-}MAC^{-1}}(56\ bits)$). Finally, the secret message must be reassembled ($T_{reassemble}$) in order to be analysed. Note also that, although Equation 8.5 reflects the total computational time devoted to process the R message repetitions, more than one RSU could be involved in the process if a hand-over occurs in between.

From the sender point of view, once the first message repetition is prepared and protected ($T^{R_0}_{prepare} + T^{R_0}_{protect}$), in order to guarantee the system's computational feasibility, the embedding of a message in the next nb_{msg} beacons ($T^{R_i}_{substitute}$) and the protection of the next one ($T^{R_{i+1}}_{protect}$) should be done in less time than that used to send those nb_{msg} beacons ($T_{nb_{msg}\ beacons}$):

$$T_{substitute} + T_{protect} \leq T_{nb_{msg}\ beacons} \tag{8.6}$$

In this way, while a previously protected message repetition R_i is being sent, the next message repetition R_{i+1} can be protected (it will be sent in the next set of nb_{msg} beacons). Otherwise, the subsequent repetitions should be put in a (potentially growing) queue. In order to estimate the sender cost, it is assumed that the most computationally significant operations are the cryptographic ones, as the remaining operations are simple manipulations of messages; therefore, $T_{substitute} \approx 0$.

To illustrate this cost, performance figures of CycurV2X (a commercial OBU[2]), provided by its manufacturer, show that the ECIES operation for 16 bytes is addressed in 27.938 ms. Although the message to protect in this work is shorter (7 bytes), we assume this performance value in our calculations, i.e., $T_{protect}$ = 27.938 ms. Recalling from Section 5.5, in our proposal $nb_{msg} = 9$. Therefore, as there is a period $T_{beacon} = 100\ ms$ between beacons, in the worst case scenario (i.e., $K = 1$) each secret message repetition takes $T_{nb_{msg}\ beacons} = nb_{msg} \cdot T_{beacon} = 900\ ms$ to be completely sent.

However, as in the proposed system it is assumed that secure beaconing is used (as a means to provide the RSUs with the public key of the reporting vehicle), the temporal overhead introduced by signature generation over sent beacons, T_{SG}, and signature verification of received beacons, T_{SV}, must be also considered. Performance figures for embedded platforms taken from [77] state that $T_{SG} = 16.856\ ms$ and $T_{SV} = 45.381\ ms$. In a $T_{nb_{msg}\ beacons}$ period, the sender will have also to spend a time $nb_{msg} \cdot (T_{SG} + \delta \cdot T_{SV})$, being δ the mean number of incoming secure beacons (i.e., signed) within a beacon period T_{beacon}. With these figures, it is obvious that a vehicle can hardly verify more than one incoming signed beacon from neighbouring

[2] https://www.escrypt.com/products/cycurv2x/details/

vehicles. To overcome this limitation, we assume that the periodic or context-adaptative verification strategies proposed in [78] are applied. Therefore, δ can be adjusted to assure that the vehicle copes with the overhead introduced by secure beaconing and leaves some time to embed the next message repetition:

$$T_{protect} + nb_{msg} \cdot (T_{SG} + \overline{\delta} \cdot T_{SV}) \leq T_{nb_{msg}\ beacons} \tag{8.7}$$

where $\overline{\delta}$ is the adjusted mean number of incoming secure beacons that will be actually verified within a T_{beacon} period. Note, however, that the mean overhead introduced by the proposed steganographic system in a T_{beacon} period is $T_{protect} \div nb_{msg} = 3.104\ ms$, which is substantially less than the overhead introduced by the secure beaconing. These assumptions make the system feasible for the sender in the worst case of the embedding interval parameter K, and as a consequence, no restrictions for this parameter exist and all its possible values could be employed.

In our scenario the entities receiving messages from all passing by vehicles will be a RSU or a set of RSUs. To assure the computational feasibility, it must be possible for a RSU to determine for the beacons sent by all passing by vehicles whether they contain an embedded message or not before the next set of beacons arrive. Considering the naïve case of only one passing by vehicle, the condition $T_{detect} < T_{beacon}$ must be hold, and the overhead introduced by secure beaconing should be also taken into account. Otherwise, it could lead to a growing queue of beacons to process. For the purpose of this work, we assume that the RSUs have enough computational capacity to make the previous condition hold. It must be noted that the ECIES time for 16 bytes is 21.26 ms in the aforementioned commercial OBU. However, the RSU's computational capacity is expected to be significantly greater than that of embedded vehicles and, moreover, the amount of data to process (i.e. the encrypted magic header) is smaller than the 16 bytes considered in such performance figure.

8.2.4 Operational feasibility

As in the proposed system it is assumed that the reporting vehicle sends the required amount of beacons while being in the range of a set of RSUs, it must be possible to send all these beacons during the time that the vehicle stays within the RSUs' range. That depends mainly on the vehicle's speed. This Section analyses the condition that must be satisfied to guarantee the system's feasibility regarding this issue. Moreover, the suitability of different system's configurations (parameters K and R) for different types of roads according to the vehicle's speed and the distance traveled is also analysed.

Assuming that a specific steganographic system is selected by choosing certain values of K and R, the required total number of beacons used to transmit a report is $N = R \cdot nb_{msg} \cdot K$. On the other hand, as beacons rate is br $(beacon/s) = 1/T_{beacon}$, the number of beacons M_{RSU} that a vehicle can actually transmit to one RSU will depend on the communication range r between both and the relative speed v of one respect to the other: $M_{RSU} = (r \cdot br)/v$ (with v in m/s and r in m). If a set of ρ RSUs are considered, the number of beacons M increases accordingly: $M = \rho \cdot M_{RSU}$.

To guarantee the system's operational feasibility, M must necessarily be greater than N. By design, $r = 1000$ m, $br = 10$ $beacon/s$ and $nb_{msg} = 9$. Therefore, the operational feasibility comes determined by:

$$R \cdot K \cdot v \leq \frac{\rho \cdot r \cdot br}{nb_{msg}} = \rho \cdot 1111,1111 \tag{8.8}$$

We analyse the system's operational feasibility in nine scenarios specified by the vehicle's speed and the distance traveled (Figure 8.2). Considered speeds are those common in highways (120 km/h), secondary roads (80 km/h) and urban environments (40 km/h). It should be noted that speeds that are over the speed limit are not considered in this analysis because it is not reasonable for an offending vehicle to report others. Concerning the distance traveled, in highways vehicles are assumed to have mean trip lengths of 60 km, 30 km and 1 km; in secondary roads, analysed mean trip lengths are 20 km, 10 km and 1 km; finally, for urban roads; 5 km, 2 km and 1 km are considered. It has been assumed that RSUs are placed every kilometre, so the number of traveled kilometers is equal to ρ. Figure 8.2 shows the probability of success $p_{success}$ in such scenarios as a function of RAB. Note that we have avoided using *exactly* some of the traveled distance values (30 km and 10 km) to increase the figure's readability.

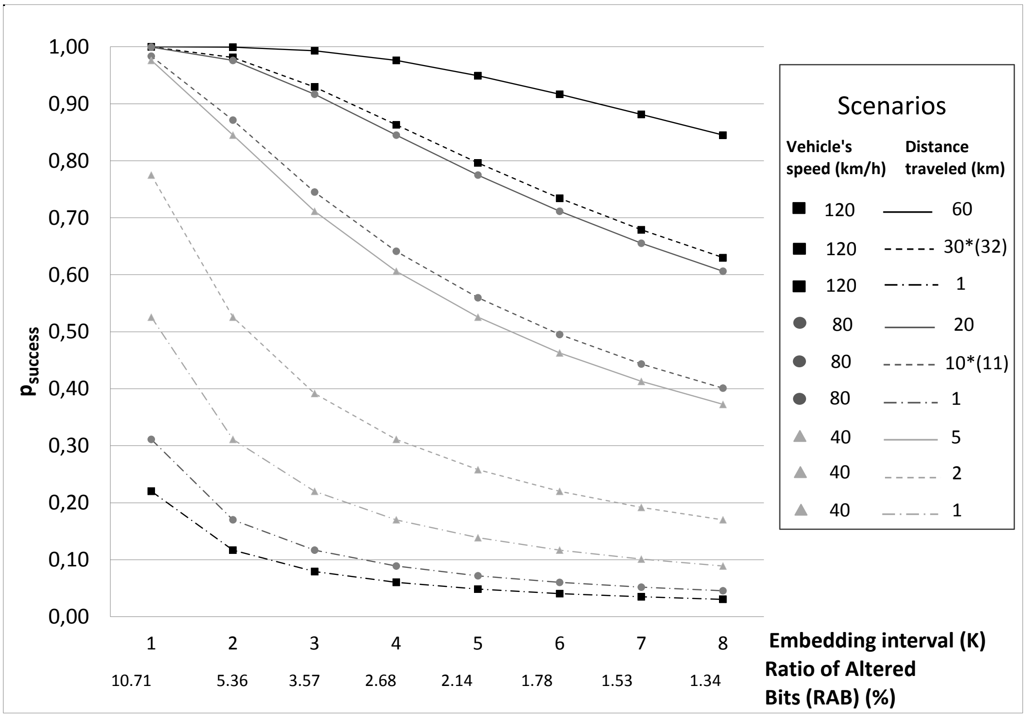


Figure 8.2: Success probability in several scenarios defined by the vehicle's speed and distance traveled

From our point of view, the system is considered to be feasible if $p_{success} \geq 0.75$. Thus, the system is not feasible if only one RSU is available (distance traveled or $\rho = 1$) for any speed value and K. If more than one RSU is considered, there is at least one feasible setting in each scenario. Generally speaking, $p_{success}$ lowers as K raises, because a higher embedding interval gives less chances to embed data for the same amount of time. Therefore, with speeds of 120 km/h, if traveled distance equals 60 km the system is feasible even if $K = 8$ ($RAB = 1.34\%$). If traveled distance equals 30 km with a speed of 120 km/h, the maximum value of K is 5, so the minimum RAB will be 2.14%. Note that the system performance is equal in this last case to the scenario where the speed is 80 km/h and traveled distance equals 20 km. in the scenario where vehicles travel at 80 km/h a distance of 10 km, the maximum value of K is 2 (RAB = 5.36%). This performance is again similar to the scenario where speed equals 40 km/h and distance 5 km, while when distance equals 2 km only one configuration presents an acceptable success probability: $K = 1$ (RAB = 10.71%).

It should be noted that in the previous calculations it has been assumed that all fragments of a given repetition are received by the intended RSU. This fact implies that there are not fragments that are not useful – it must be recalled that all fragments of a given repetition are encrypted for a given RSU, so they could not be decrypted by another one. This assumption is in line with the working assumption presented in the model (recall Section 5.2.3).

8.2.5 Requirements analysis

In this Section, it is evaluated the achievement of the requirements imposed in Section 5.2.2. It should be noted that the requirement of computational feasibility for both the sender and the receiver has already been analysed in Section 8.2.3. Similarly, the resistance against data losses has been studied in Section 8.2.2.

Concerning the embedded message integrity, it must be noted that it has been assumed that the cover message (beacon) is digitally signed. Furthermore, the secret message structure already contains a message authentication code that enables detecting manipulations over the embedded data. Therefore, any variation on the message will be detected by the receiver. As the cover message in the proposed mechanism are beacons, and given that such messages are not routed, it is not possible for third parties to perform intentionally this threat.

The following subsections focus on the other two requirements, undetectability and maximum capacity, which require an in-depth discussion.

Undetectability

In the context of the studied domain, the detection of steganography may be interesting for some of the VANET participants. As VANET messages are transmitted through a shared channel, unintended recipients (particularly, the reported driver) are able to eavesdrop its content, potentially allowing them to discover the covert channel. Given that the secret message is encrypted before embedding, unauthorized receivers will not be able to access its content. However, it can allow them to detect the use of steganography by discovering statistic anomalies in the distribution of the least significant bits of the data elements involved in covert channel communications [79]. This technique is widely used to attack Least Significant Bit (LSB) steganography in images [80]. It has been assumed that sensor inaccuracies are random and according to the sensor accuracy and resolution (recall Section 5.1). Therefore, the resolution and accuracy of beacon fields data have been used to measure the amount of data that is possible to embed without disturbing the sensor measures outside the allowed boundaries. Nevertheless, a practical evaluation with real sensors on a real scenario should be performed. Therefore, it is not possible to ensure that errors produced by sensor measures are truly random. This fact could be used to ease the covert message detection.

There are two factors that make such attack difficult. On one hand, the proposed steganographic system is parametrized in such a way that only a portion of messages may include secret information. In this way, statistical anomalies will be masked by the natural properties of messages with no embedded information. On the other hand, it must be noted that vehicles use temporary identifiers (pseudonyms) to avoid the chance of tracking [54]. As a consequence, it makes difficult (specially in dense roads) to discover all messages generated from the same vehicle. Both factors reduce dramatically the amount of information available to an attacker. Additionally, to reduce the amount of statistical changes introduced to sensor measurements, it would be possible to reduce the amount of least significant cover bits used to embed data.

Apart from the previous considerations, it should be noted that the detection of the embedded data by a timing attack may not be performed in this scenario. Thus, current standards impose that the beacon message be sent every 100 ms. In this situation, it is not possible to determine whether a given beacon contains embedded data or not, as this operation does not affect to the moment in which it has to be sent.

Maximum capacity

The proposed mechanism is designed in such a way that it uses the maximum capacity that is enabled by the current precision and accuracy. Therefore, as using a greater capacity would affect the reliability of the sensorial data at stake, it is not possible to use a greater capacity on each beacon. Despite this fact, the embedding interval K impacts negatively on the global capacity of the system, as only one out of K beacons is enabled to contain embedded data. However, thanks to this interval the undetectability is improved. At the light of this facts, it may be concluded that the system offers the maximum capacity while remaining practical and reasonably undetectable.

It must be noted that there are two ways to reduce the covert channel capacity as it is currently defined. First, if the technology developments increase the accuracy of sensors, it is expected that the underlying standards may evolve in the same direction, thus reducing the measure uncertainty which is used to embed data. The threat of this initiative into the proposed scheme is thus dependent on the technological evolution and its standardisation. Second, a malicious vehicle may overload the VANET with messages, in order to avoid other vehicles to use the network. The impact of this alternative is relatively low, as several research contributions (such

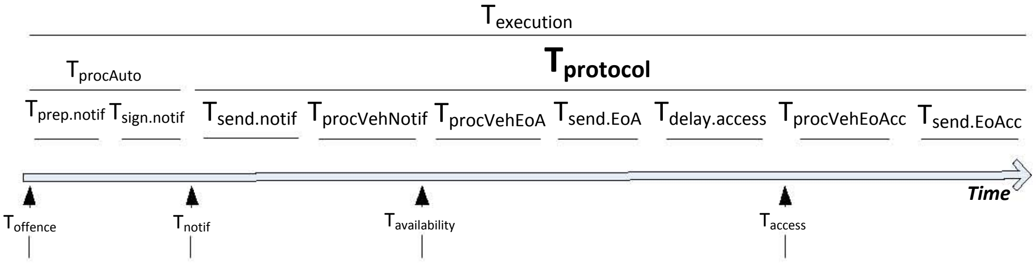


Figure 8.3: Temporal evolution of the considered process

as the LEAVE protocol [67]) have already focused on this issue.

8.3 Evaluation of the notification protocol

In this Section, the proposed vehicular-enhanced notification protocol is evaluated. First (Section 8.3.1), the practical applicability of the proposed mechanism is analysed, considering a realistic vehicular scenario.

From the Authority viewpoint, the process efficacy is expressed in terms of the total time taken (i.e. the lower such time is, the greater the efficacy the process has). Such time (t$_{execution}$) will be the sum of the time taken by the Authority to prepare the notification (t$_{procAuto}$) and the time taken by the proposed mechanism to send it (t$_{protocol}$) (Figure 8.3).

Thus, this analysis aims to characterize t$_{protocol}$ in order to show how it may contribute to the aforementioned goal. Section 8.3.1 analyzes t$_{protocol}$ but to a limited scope: only the vehicular network scenario is considered – the interaction with DRA is out of the scope, as there may exist an intrinsic delay. Such delay is the time taken to arrive to the place in which the reliable channel is established (e.g. parking lot), which is not foreseeable (i.e. it may range from a few minutes to a couple of hours or days).

The last part of Section 8.3.1 aims to determine whether the use of RSUs is suitable for this protocol. It should be noted that all messages (notification and evidences of availability and access) should be exchanged with *the same* RSU, as it is the Notification Sender. Otherwise, the proposed approach would only be suitable for scenarios in which RSUs where interconnected, or in which the Notifier where accessed through other communication media (e.g. GSM channel). According to Figure 8.3, most components of $t_{protocol}$ are related to data processing or transmission. However, there is one component, $t_{delay.access}$, which is the time until the driver accesses to the notification. This action must happen when it does not disturb the driver, which may happen immediately (e.g. if driving in sparse traffic conditions in a calmed environment) or after some time (e.g. if driving in rush hours). Therefore, it is required to know the maximum value of $t_{delay.access}$ that ensures that the protocol may be fully executed in this scenario. Such issue is studied in Section 8.3.1.

Finally, Section 8.3.2 analyses the achievement of the security requirements derived from the legal framework.

8.3.1 Performance evaluation

The time to execute the whole protocol ($t_{protocol}$) is composed by seven factors (Figure 8.3). Two are related to the notification (step 1 of the protocol) – the time to send it ($t_{send.notif}$), and the time required by the vehicle to process it ($t_{procVehNotif}$). Other two are related to the evidence of availability, the second step of the protocol ($t_{procVehEoA}$ to prepare it and $t_{send.EoA}$ to send it). There is a delay time $t_{delay.access}$, which is the time taken by the driver to access to the notification. Finally, there are two factors related to the evidence of access (step 3 of the protocol), $t_{procVehEoAcc}$ for its preparation and $t_{send.EoAcc}$ for its transmission.

Based on its definition, the proposed protocol is only successful when all messages have been exchanged. However, in the vehicular context the sending unit (i.e. the OBU) may be compromised in such a way that it does not send back the evidences. The impact of the compromise of OBUs over the performance is analysed in the following subsection of this Section.

Despite the threat of OBU compromise, it should be noted that such misbehavior will be easily identifiable through the use of the resilient channel. Thus, even if it is a realizable threat, it is assumed that its real presence will be very low. Thus, for the remaining performance calculations, it will be assumed that OBUs are not compromised.

In order to measure the performance of the protocol, the time taken will be measured. Speaking generally, the time to send a message is determined by the time taken for the transmission, along with that required to manage the retransmissions to contribute on countering the channel unreliability. On the other hand, the processing time of the in-vehicle device is determined by its computational resources. The time to send the studied messages is analyzed in the second subsection of this Section. Afterwards, the processing time of the in-vehicle device is studied in the last subsection.

Impact of the degree of OBUs compromise over the performance

The value $p_{succ.notif}$ is the probability of a given execution of the protocol to be successfully finished over the vehicular network. In the proposed protocol, such success is achieved when both the notification and the respective evidences of availability and access are successfully received. The event of receiving each message is subject to its own probability, namely $p_{rcv.notif}$, $p_{rcv.eoa}$ and $p_{rcv.eoacc}$. However, in the case of evidences, it may also happen that they are not sent, as a result of being compromised. Thus, $p_{not.comprom}$ is the probability for an OBU of not being compromised. It is assumed that in case of compromise, neither of the required evidences (i.e. availability and access) is sent by the OBU. Based on this four probabilities, and given that all events are independent each other, $p_{succ.notif}$ may be written as follows (Equation 8.9).

$$p_{succ.notif} = p_{rcv.notif} \cdot p_{rcv.eoa} \cdot p_{rcv.eoacc} \cdot p_{not.comprom} \tag{8.9}$$

In this analysis, it will be assumed that the transmission probabilities are equal for all messages (commonly referred to as $\mathrm{p}_{rcv.msg}$), thus leading to Equation 8.10.

$$p_{succ.notif} = p_{rcv.msg}^{3} \cdot p_{not.comprom} \tag{8.10}$$

Taking into account that $\mathrm{p}_{rcv.msg} \leq 1$ by definition, the previous Equation may be rewritten as follows (Equation 8.11):

$$p_{rcv.msg} = \sqrt[3]{p_{succ.notif}/p_{not.comprom}} \leq 1 \tag{8.11}$$

According to the previous expression, it may be seen that it only holds if $\mathrm{p}_{succ.notif} \leq \mathrm{p}_{not.comprom}$. This condition has a direct interpretation in this context – the degree of unreliability of OBUs will determine the maximum amount of success that the proposed protocol will have over any not-resilient channel. Considering that 25% of OBUs are compromised (i.e. $\mathrm{p}_{not.comprom} = 0.75$), this means that over 100 executions of this protocol, 25 of them will not be successful, as compromised OBUs will never send back the corresponding evidences. With respect to the remaining 75, their success will be conditioned by the reliability of the channel. Thus, if the protocol is executed over a reliable channel, all of them will be successful. On the contrary, if the channel does not ensure that packets are successfully delivered (as it is the case of the wireless vehicular network), the amount of successful executions may be low due to the data loss in the communication channel. In order to counter the unreliability of the vehicular communication channel, both the notification and the evidences will be retransmitted several times. The analysis of this retransmission strategy and its impact over the transmission time is presented in the following subsection.

Analysis of $\mathbf{t}_{send.notif}$, $\mathbf{t}_{send.EoA}$ and $\mathbf{t}_{send.EoAcc}$

In this Section, the values of $t_{send.notif}$, $t_{send.EoA}$ and $t_{send.EoAcc}$ are analysed under the assumption that OBUs are not compromised. In order to counter the unreliability of the vehicular communication channel, all messages are re-sent a number α of times. Such parameter is established based on the probability of success $p_{succ.notif}$ – the bigger the number of retransmissions, the bigger the probability of a message to arrive to its destination (except in the case that the probability of sending a single message is null).

$P_{rcv.msg}$ is, in the presence of retransmissions, the probability that at least one retransmission arrives. According to [74], the probability of receiving a message that has been repeated α times is related to the probability $p_{succ.rep}$ of successfully receiving each repetition. Such relationship is given by the following expression (Equation 8.12).

$$p_{rcv.msg} = 1 - (1 - p_{succ.rep})^{\alpha} \tag{8.12}$$

Combining this expression with the one provided for $p_{rcv.msg}$ (Equation 8.11), under the assumption of $p_{not.comprom} = 1$, enables finding a relationship between the amount of retransmissions and the probability of success based on the probability of receiving each repetition:

$$\alpha = \lceil log(1 - \sqrt[3]{p_{succ.notif}})/log(1 - p_{succ.rep}) \rceil \tag{8.13}$$

According to [74], $p_{succ.rep} = 0.58$ for a vehicle-to-vehicle communication separated by 400 meters. Using such parameter, the evolution of the required amount of retransmissions based on a predefined probability of success can be studied (Figure 8.4). Thus, for a $p_{succ.notif} = 0.99$, every message must be re-sent 6,57 times (more precisely, 7 times, as the number of repetitions must be natural), whereas for $p_{succ.notif} = 0.75$ this number is decreased to 2,75 times (i.e. 3 repetitions).

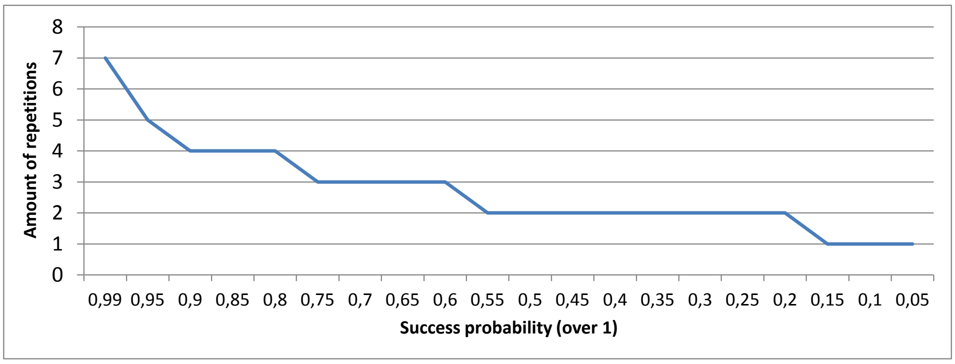


Figure 8.4: Evolution of the amount of retransmissions based on the success probability

Based on the amount of retransmissions, it is possible to determine the total time required to send each of the considered messages. Such time is the sum of the times required for each retransmission, thus leading to the following expressions:

$t_{send.notif} = \alpha \cdot t_{transm.notif}$,

$t_{send.EoA} = \alpha \cdot t_{transm.EoA}$

$t_{send.EoAcc} = \alpha \cdot t_{transm.EoAcc}$

The transmission time for each message ($t_{transm.notif}$, $t_{transm.EoA}$ and $t_{transm.EoAcc}$) is determined by two factors – the time for the sender to transmit the message (*transmission delay*) and the time to propagate it in the network (*propagation delay*). In this context, the propagation delay is negligible, as it is calculated as d/s where d is the distance from sender to receiver (up to 1 kilometre due to DSRC maximum range [81]) and s is the speed of light (in any wireless scenario). Thus, such delay is $1(km)/300000(km/s) \approx 0$.

Concerning the transmission delay, it is determined by the message size and the channel bandwidth. Tables 6.2, 6.3 and 6.4 describe the sizes for each message (404, 217 and 218 bytes, respectively). On the other hand, the channel bandwidth for a DSRC channel is 6 Mbps [81]. Using both data, the time required to perform the retransmissions (for each value of $p_{succ.notif}$) is shown on Figure 8.5. Thus, for a $p_{succ.notif} = 0.99$,

$t_{send.notif} = 7 \cdot 404$ (bytes) / 750000 (bytes/sec) = 0.004 seconds,

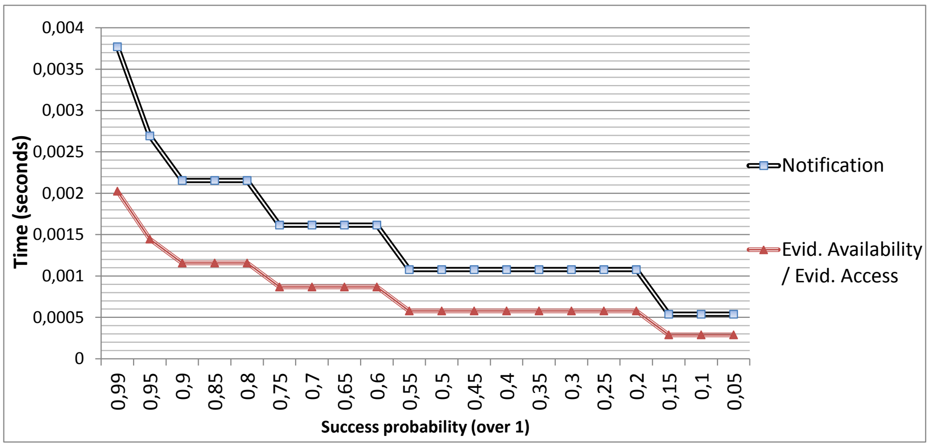


Figure 8.5: Transmission times for the considered messages based on the probability of success

$t_{send.EoA}$ = 7 · 217 (bytes) / 750000 (bytes/sec) = 0.002 seconds, and

$t_{send.EoAcc}$ = 7 · 218 (bytes) / 750000 (bytes/sec) = 0.002 seconds.

Analysis of $\mathbf{t}_{procVehNotif}$, $\mathbf{t}_{procVehEoA}$ and $\mathbf{t}_{procVehEoAcc}$

Cryptographic operations are the most significant processing tasks for the vehicular device. Other basic tasks (e.g. message queueing, discarding repeated messages, change of context to work on other ITS services, etc.) are assumed to have a negligible cost with respect to these operations. Particularly, the vehicular device has to decrypt the notification message and verify its signature. Concerning the evidences of availability and access, it has to sign and encrypt them.

In order to illustrate the time taken by the aforementioned operations, the performance offered by a commercial vehicular device (CycurV2X) is considered. Such device encrypts 16 bytes in 27.938 ms (21.26 ms. required for decryption). Digital signature for such data is done in 7.156 ms. whereas the verification requires 27.114 ms. This last figure does not include the time (referred to as σ_v) to verify the public key certificate status. Nevertheless, in the following calculations it will be assumed that the Message Issuer certificate is already verified (i.e. $\sigma_v = 0$) before the vehicular device starts functioning. It is a reasonable assumption since this is a well-known entity.

As the data at stake in this protocol is significantly bigger than that considered by the previous performance figures, it is necessary to adapt them for the current message length. Such adaptation depends on the very nature of the algorithm. For encryption, the ECIES algorithm is based on a stream cipher that uses a symmetric key. Such key is encrypted using public key cryptography. Thus, the most significant operation is the public key encryption, and it is assumed that the cost of the stream cipher is linearly proportional to the message length. Concerning the signature, ECDSA encrypts asymmetrically the result of a hash function over the considered message. As the result of such function is always of the same length, having a greater message only imposes a greater cost over the hash function. As the hash function usually divides the message in blocks of the same amount of bytes, the difference in performance will be based on the difference between the amount of blocks. For the following calculations, the SHA-256 hash function will be considered. Such function uses a block size of 64 bytes.

Taking into account the previous considerations, processing the notification message takes

t$_{procVehNotif}$ = t$_{decrypt.notif}$ + t$_{verif.notif}$ = 21,26 (ms / block of 16 bytes) · ratio$_{decrypt}$ + 27,114 (ms / block of hash function) · ratio$_{verif}$, where

ratio$_{decrypt}$ = ⌈ 404 bytes (notif) / 16 bytes (reference implementation) ⌉ = 26 blocks of 16 bytes

ratio$_{verif}$ = ⌈ 223 bytes to verify (notif) / 64 bytes per block of hash function ⌉ = 4 blocks of hash function.

In the previous calculations, the amount of bytes to decrypt is the whole notification message (i.e. 404 bytes), whereas the data to verify are 223. In the first case, the whole notification message, including the public key certificate and the signature, are encrypted. These data are not part of the data to verify. Using the obtained values t$_{procVehNotif}$ may be calculated as follows:

$t_{procVehNotif} = t_{decrypt.notif} + t_{verif.notif} = 21.26 \cdot 26 + 27.114 \cdot 4 = 661.2$ ms $= 0.661$ s.

In an analogous way, for the evidence of availability,

$t_{procVehEoA} = t_{signEoA} + t_{encryptEoA} = 7.156$ (ms / block of hash function) $\cdot$ ratio$_{sign}$ + 27.938 (ms / block of 16 bytes) $\cdot$ ratio$_{encrypt}$, where,

ratio$_{sign}$ = $\lceil$ 36 bytes to sign (evid. of availability) / 64 bytes per block of hash function $\rceil$ = 1 blocks of 64 bytes

ratio$_{encrypt}$ = $\lceil$ 217 bytes (notification) / 16 bytes (reference implementation) $\rceil$ = 14 blocks of 16 bytes

Using these values, the time to process the evidence of availability can be calculated,

$t_{procVehEoA} = 7.156 \cdot 1 + 27.938 \cdot 14 = 398.288$ ms $= 0.398$ s.

For the sake of brevity, it may be seen that $t_{procVehEoAcc} \approx t_{procVehEoA}$, as both evidences have a very similar size (only one byte of difference) and the cryptographic operations are the same. Using these values of $t_{procVehNotif}$, $t_{procVehEoA}$ and $t_{procVehEoAcc}$ it is possible to calculate the total time that the vehicular device takes for processing these messages:

$t_{procVehicle} = t_{procVehNotif} + t_{procVehEoA} + t_{procVehEoAcc} = 0.661 + 0.398 + 0.398 = 1.457$ s.

Analysis of $t_{delay.access}$. Discussion on its impact over the suitability of RSU-based communications for this protocol

The time $t_{delay.access}$ that a driver may need to access to the notification is affected by the driving situation. However, such value is critical to ensure that the whole protocol may be executed using a single RSU – if the vehicle at stake gets out of range of the RSU[3] when all messages have not been exchanged, then the protocol

[3] In this evaluation, only direct communication between vehicle and RSU is considered. The use of routing strategies that could increase the reachability of the vehicle are not considered, as this issue is a matter of open research and thus the results could be conditioned by the routing strategy selected.

will need the resilient channel to be finished. As the use of such channel introduces a delay in the process (the time required to arrive to where the channel is available), it is advisable to minimize as much as possible the need of such alternative.

In order to ensure that all messages are exchanged while the vehicle is in RSU's range, it is necessary to determine how long the vehicle is within this area. Thus, considering a maximum speed of 120 km/h, and given that the range is 1 kilometre [81], the vehicle is 1 (km) / 120 (km/h) = 0.0083 h = 30.0 seconds in range. Taking into account this value,

$\mathrm{t}_{protocol} = \mathrm{t}_{send.notif} + \mathrm{t}_{procVehNotif} + \mathrm{t}_{procVehEoA} + \mathrm{t}_{send.eoa} + \mathrm{t}_{delay.access} + \mathrm{t}_{procVehEoAcc} + \mathrm{t}_{send.EoAcc} \leq 30.0$

According to the previous expression, and taking into account the values for computation and transmission for messages previously calculated in this Section, $\mathrm{t}_{delay.access}$ must fulfil the following condition in order to ensure the suitability of RSUs in this scenario:

$\mathrm{t}_{delay.access} \leq 30.0 - 0.004\ (\mathrm{t}_{send.notif}) - 0.661\ (\mathrm{t}_{procVehNotif}) - 0.398\ (\mathrm{t}_{procVehEoA}) - 0.002\ (\mathrm{t}_{send.eoa}) - 0.398\ (\mathrm{t}_{procVehEoAcc}) - 0.002\ (\mathrm{t}_{send.EoAcc}) = 28.535$ seconds.

At the light of this value, the driver has around 28 seconds to access to the notification. It should be noted that in case of speeding offences, the vehicle may be driven at a higher speed, say 199 km/h in a highway[4]. Using this value, the vehicle would be 1 (km) / 199 (km/h) = 0.005 h = 18.09 seconds in range, which leads to a delay for accessing of

$\mathrm{t}_{delay.access} \leq 18.09 - 0.004\ (\mathrm{t}_{send.notif}) - 0.661\ (\mathrm{t}_{procVehNotif}) - 0.398\ (\mathrm{t}_{procVehEoA}) - 0.002\ (\mathrm{t}_{send.eoa}) - 0.398\ (\mathrm{t}_{procVehEoAcc}) - 0.002\ (\mathrm{t}_{send.EoAcc}) = 16.625$ seconds.

An extended analysis should be conducted to ensure which driving conditions might allow this delay on the driver. In any case, it should be noted that such time is increased with the reduction of the driving speed. In fact, such value could be used by the Authority to estimate whether it will be feasible for the driver to take

[4] Even if the speed could be higher, according to the Spanish legal framework driving at 200 km/h in a highway is considered a crime, and it is thus processed using the criminal law. Such process is out of the scope of this thesis.

this decision based on the current traffic status data, obtained for example through the use of other ITS-related applications such as *floating car data* [82]. Based on such estimation, other communication channels (e.g. GSM connection) could be selected.

8.3.2 Security requirements analysis

Table 8.5 summarizes the achievement of the imposed requirements. At the end of the notification process, there are three possible final status – the notification has been delivered through the vehicular communication, or through the reliable channel by means of the DRA, or it has not been delivered. In all situations, either NMan or the DRA have enough elements to attest the situation. In the first case, NMan has the evidence of availability which is signed by NRS. If such evidence was not successfully verified or simply not received, the resilient channel (with the DRA) is employed. This entity may either (1) have such evidence correctly verified or (2) do not have any valid data. In this second scenario, DRA is entitled to attest the situation because (1) it is a trusted entity and (2) the underlying channel was resilient to send the information. Thus, although the protocol may finish with NR having the notification while NMan / DRA do not have a valid evidence of availability, these entities are able to detect the situation, to take the appropriate corrective actions (i.e. call for maintenance) and to proceed with other notification mechanism. Based on these facts, requirement Req1 is fulfilled.

A similar situation happens with the attestation of access (Req2). However, in this case only two situations are possible – if NMan or DRA do not receive the corresponding evidence in a predefined interval, the legislation establishes that the notification has been successfully performed. Thus, either an evidence of access (i.e. evidence of non-repudiation of delivery) is explicitly received or, in its absence, a default evidence (of implicit rejection) may be created.

Concerning the NRS authenticated access control (Req3), it is ensured by the need for a password (recall step (0)) to enable the NRS as a suitable notification place. The underlying security of the in-vehicle devices (particularly, its HSM) ensures that such activation is only performed by introducing this password. It must be noted that the proposed mechanism only ensures that *somebody that knows the password* accesses to the notification. Additional authentication mechanisms (such as biometry-based approaches) should be introduced here to ensure that such person is indeed the driver. Such issue is identified as a future research work.

The availability of the notification system (Req4) may not be ensured without a practical analysis in a real device. Even if the Notifier is assumed to be available (as RSUs have enough computational resources, by assumption), neither the communication channel or the NRS are assumed to be available. The performance analysis of Section 8.3.1 is intended to illustrate this issue. Similarly, from the theretical point of view it is not possible to ensure the physical access control requirement (Req5). Even if the in-vehicle devices are protected to some extent (as they are installed inside the vehicle), RSUs are publicly accessible and thus they require some additional protective mechanisms.

Concerning the synchronization of the notification system (Req6), both NP and NRS have their reliable time sources. NP may have access to it (e.g. the time server from the Spanish Real Observatorio de la Armada) through the network infrastructure, whereas the in-vehicle platform may use the one of the HSM.

The authentication of the notification (Req7) is ensured thanks to the MI's electronic signature. Such mechanism also enables to verify the message integrity (Req9). On the other hand, the message confidentiality (Req8) is ensured thanks to the use of the public key encryption. It must be noted that NP is not able to access to the notification as the encryption is performed directly by MI in step (1).

Requirement	**Fulfilment status**
Req1 (Non-repudiation of receipt)	Achieved
Req2 (Non-repudiation of delivery)	Achieved
Req3 (Authenticated access control to NRS)	Achieved
Req4 (Availability of the notification system)	Unclear (implementation required)
Req5 (Physical access control)	Unclear (implementation required)
Req6 (Synchronization)	Achieved
Req7 (Message authentication)	Achieved
Req8 (Confidentiality of the notification)	Achieved
Req9 (Integrity of the notification)	Achieved

Table 8.5: Summary of the fulfilment of the requirements imposed over the proposed notification protocol

8.4 Evaluation of EVIGEN

In this Section, the proposed mechanism is assessed using three ways. First, in Section 8.4.1 it is analysed whether it conforms to the evidence management cycle defined in Section 3.3.2. Second, a performance evaluation is shown in Section 8.4.2. Finally, the fulfilment of the imposed requirements is analysed in Section 8.4.3.

8.4.1 Conformance to the evidence management cycle

The evidence management cycle is composed by six consecutive steps that, in general words, are mostly addressed by the proposed protocol.

Concerning the design of the evidence, it is fulfilled by the description of the contents of the evidence and also of its header and the testimonies contained in it. The creation of the evidence is also described in the protocol, detailing the specific process that the Evidence Manager should follow. As a difference to the traditional management cycle, there is no need to perform a real collection step, as the entity that generates the evidence is the same that has to perform the following step – the evidence analysis. Particularly, it has been defined as part of the creation process, that at least one testimony should be supporting the requester claim. Such procedure (which avoids the creation of non-relevant evidences) is the essence of the evidence analysis step.

Once it has been created, the evidence is presented to the adjudicator (evidence report and presentation step). This entity is in charge of performing the evaluation of the evidence, which is partially addressed in the proposed contribution through the evidence verification procedure. The future decision process on the relevance of the evidence for the enforcement action is out of the scope of this contribution.

8.4.2 Performance evaluation

In this Section, the performance of the proposed approach is evaluated. Due to the unreliability of the vehicular network, the high mobility of vehicles and their limited computational resources, the more challenging environment is the vehicular one. Therefore, this analysis will focus on how the protocol performs in such environment. Particularly, two indicators will be considered, namely (1) the computational and storage cost for vehicles and the impact in the vehicular network (analysed in the three first subsections of this Section) and (2) the amount of evidences, and testimonies per evidence, that may be achieved in a road scenario (analysed in the last subsection of this Section). For the second indicator, it must be noted that the time interval between the offence and the notification may have a critical impact over the protocol effectiveness – it may cause witnesses to be non reachable for R, due to their high mobility.

Vehicular computational and network cost

In order to give a lower bound for this cost, this analysis only considers *ideal* conditions, that is, there are not external computational workloads derived from other ITS simultaneous applications, which could cause delays to the protocol at stake. Particularly, the cost of performing and verifying the signatures over beacons will not be considered. Furthermore, for these calculations it should be recalled that the proposed protocol, as a difference with contributions C2 and C3, does not contain any strategy of repeating several times each of the exchanged messages to counter the vehicular network unreliability (recall Section 7.1).

Prior to estimate the costs, it is necessary to define the computational and network available resources. Concerning the computational platform, a commercial vehicular HSM (CycurV2X[5]) is considered. Although there are delays introduced by the OBU's and SAE's processing, as well as the in-vehicle communication network, it is estimated that the most costly operations are related to cryptographic calculations. Thus, only such operations will be considered in this analysis. According to figures provided by its manufacturer, CycurV2X performs ECIES encryption of 16 bytes in 27.938 milliseconds (21.26 ms. for decryption). Regarding the ECDSA signature operation, it is performed in 7.156 ms. (27.114 ms. for its verification, plus a time of σ_v to verify the public key certificate status). Both ECIES and ECDSA are selected for compliance to the current standard in security of vehicular networks (IEEE 1609.2, [8]).

Related to the network resources, a typical inter-vehicle DSRC (Dedicated Short Range Communications) network is considered. Such network has a bandwidth of 6 Mbps [81]. Even if a different network technology will be used for the resilient network (to execute the exception handling processes), the same bandwidth will be assumed.

Taking into account these figures, Table 8.6 details the cryptographic operations for each algorithm and summarizes their processing costs. Note that the provided performance data are referred to 16 bytes, but the data structures have a different size. Thus, it is necessary to extrapolate these values for each size, which depends on the cryptographic algorithm design. In the case of ECIES encryption, it is an hybrid encryption scheme – it uses the public key to create a ciphering sequence, which is the input key for a stream cipher. Such type of encryption does not divide

[5] https://www.escrypt.com/products/cycurv2x/details/, accessed in January 2012.

Algorithm	**Cryptographic operations**	**Vehicular process. time (ms)**
Testim. Collection (REQ)	2 sign. (req.) + $nw \cdot$ encrypt (req.)	$14.31 + nw \cdot 670.51$
Testim. Collection (WIT)	1 decrypt (req.) + 2 sign. verif. (req.) + 1 sign. (testim.) + 1 encryption (testim.)	$708.1 + 2 \cdot \sigma_v$
Evid. Generation (REQ)	1 sign. (evid. header) + 1 encrypt (evid. header) + 1 sign. verif. (evid. header ack)	$341.59 + \sigma_v$
Evid. Verification	None (performed by Adj)	0
Testimony Excep. Handling	1 decrypt (testim. enquiry) + 1 sign verif. (testim. enquiry) + 1 encrypt (testim.) + 1 sign. (testim.)	$216.21 + \sigma_v$
Evidence Header Excep. Handling	1 sign. (evid. header) + 1 encrypt (evid. header) + 1 sign. verif. (evid. header ack)	$341.59 + \sigma_v$

Table 8.6: Summary of processing times for each algorithm. nw is the number of participant witnesses. σ_v is the time to verify a public key certificate

the message in blocks, so it is reasonable to estimate that there will be a linear relationship between the message size and the encryption time. On the other hand, ECDSA signature is based on hash functions. According to IEEE 1609.2, such function has to be SHA-224 or SHA-256 ([8]). As it uses a message block size of 64 bytes, which is greater than the messages to sign by the vehicle (see Table 8.7), we will consider that the signature time is the same in all cases.

The operations for R concerning the testimony collection take a variable time, as it depends on the amount of witnesses nw – the request is encrypted individually for each W$_i$. Concerning the witness, it must be noted that Algorithms 8 and 10 (recall Section 7.4) have different workloads, even if their purpose is the same (i.e. to prepare the testimony). In Algorithm 8, there is a need to encrypt not only the request, but also the public key certificate of R(t$_{off}$) for privacy purposes, as explained in Section 7.4.4. The witness has to decrypt these data and, moreover, the request includes two signatures to be verified. Both issues are different to Algorithm 10, where the message is smaller and the public key certificate is not encrypted as the EM does not need to protect its privacy. Regarding Algorithm 9, there is no computation workload on the vehicle as it is fully performed by Adj. Finally, the workload for the requester in the evidence generation is related to the evidence header. Thus, it has to prepare (i.e. sign and encrypt) this data structure and to verify the corresponding acknowledgement by its receiver. This workload is the same as in the Evidence Header Exception Handling procedure (Algorithm 11).

Regarding the transmission costs, there are two relevant factors – the propagation delay and the network transmission one. The propagation delay ($T_{propagation} = distance$ / *wave propagation speed*) is assumed to be negligible. In particular, for wireless environments the wave propagation speed is the speed of light (300.000 kms / s), whereas the distance between sender and receiver is in the order of a few kilometres. In fact, even if the communication range of DSRC is one kilometre, there may be a multi-hop communication between both communicants. Thus, for a *distance* = 10 kms. , $T_{propagation}$ = 3,33 * 10^{-5} seconds ≈ 0.

To calculate the network transmission delay, it is necessary to determine each message's size. For this purpose, Table 8.7 shows the size for each data element. Based on these data, Table 8.8 summarizes the data sent on each algorithm, along with its transmission time. Thus, all transmission times are lower than a millisecond, except from Algorithm 8, which depends on the amount of witnesses nw. It should be noted that the absence of retransmissions makes this time significantly shorter than the transmission time of the notification protocol (recall Section 8.3.1).

Using the previous values, it is possible to determine the total time taken since the first request is prepared and until the evidence is ready to be created. For such calculation, the worst case will be assumed, that is, all operations are performed sequentially. It happens when the evidence header is sent after the testimony, so there are no parallel operations. There are four cases: when there is no exception, when there is a testimony exception, an evidence header exception or both of them. Equation 8.14 shows the expression for all cases, considering a single witness.

Data element	**Size (bytes)**
Public key certificate	125 ([78])
Digital signature	56 ([78])
Vehicle identifier	4 ([59])
Behavior-related variable estimation	10 (position: latitude, longitude and elevation), 2 (speed) ([59])
Time mark	2 ([59])
Offence identifier	4 (estimated by us)
Acknowledgement	4 (estimated by us)

Table 8.7: Size of data elements

Algorithm	**Sent data**	**Transmission time (ms)**
Testim. Collection (REQ)	$nw \cdot$ (Request + 2 certificate)	$0.47 \cdot nw$
Testim. Collection (WIT)	Request + 2 certificate + testimony + certificate	0.73
Evid. Generation (REQ)	Evidence header + certificate + acknowledgement + offence identifier	0.52
Evid. Verification	None (internal process of Adj)	0
Testimony Excep. Handling	Beacon + offence identifier + vehicle identifier + time mark + certificate + testimony + certificate	0.53
Evidence Header Excep. Handling	Evidence header + certificate + acknowledgement + offence identifier	0.52

Table 8.8: Summary of transmission cost per algorithm

$$T_{evid\text{–}gen} = T_{request} + T_{testimony} + T_{evid\text{–}header} + T_{exceptions} \tag{8.14}$$

T$_{request}$ (see Equation 8.15) is the time taken for a request to be created (T$_{crypto\text{–}request\text{–}requester}$), sent to a witness (T$_{send\text{–}request}$) and processed by this entity (T$_{crypto\text{–}request\text{–}witness}$).

$$T_{request} = T_{crypto\text{–}request\text{–}requester} + T_{send\text{–}request} + T_{crypto\text{–}request\text{–}witness} \tag{8.15}$$

On the other hand, T$_{testimony}$ (see Equation 8.16) is the time taken by the witness to prepare the testimony (T$_{crypto\text{–}testimony}$) and to send it to EM (T$_{send\text{–}testimony}$). Similarly, T$_{evid\text{–}header}$ (Equation 8.17) is the time taken by the requester to create (T$_{crypto\text{–}evidHeader}$) and to send (T$_{send\text{–}evidHeader}$) the evidence header.

$$T_{testimony} = T_{crypto\text{–}testimony} + T_{send\text{–}testimony} \tag{8.16}$$

$$T_{evid\text{–}header} = T_{crypto\text{–}evidHeader} + T_{send\text{–}evidHeader} \tag{8.17}$$

Finally, T$_{exceptions}$ (see Equation 8.18) is the time taken to proceed with the exception handling procedures. Particularly, T$_{establish\text{–}resilient\text{–}channel}$ represents the time until the resilient channel is available for the vehicle. T$_{send\text{–}enquiry}$ + T$_{crypto\text{–}enquiry}$ represents the time to send and to process the request for testimonies (in the Testimony Exception Handling procedure). On the other hand, $ExceptionTestim$ and $ExceptionEvHeader$ are boolean values that have value 1 when it is necessary to execute the Testimony Exception Handling procedure and the Evidence Header Exception Handling one, respectively. The remaining components of Equation 8.18 are already defined in the previous equations.

$$\begin{aligned}T_{exceptions} &= ExceptionTestim \cdot (T_{establish-resilient-channel} + T_{send-enquiry} + \\ &+ T_{crypto-enquiry} + T_{crypto-testimony} + T_{send-testimony}) + ExceptionEvHeader \cdot \\ &\cdot (T_{establish-resilient-channel} + T_{send-evidHeader}) \qquad (8.18)\end{aligned}$$

In case that an exception happens, it is necessary to wait for the resilient channel to be available. As it typically means the time to arrive to the physical place where such channel exists, there is no reasonable estimation for this value (i.e. T$_{establish-resilient-channel}$). For this reason, in this analysis only the case with no exceptions will be considered. In such a case, the former expression is simplified as follows:

$$\begin{aligned}T_{evid-gen} &= T_{request} + T_{testimony} + T_{evid-header} = \\ &= T_{send-request} + (T_{crypto-request-requester} + T_{crypto-request-witness} + \\ &+ T_{crypto-testimony}) + T_{send-testimony} + T_{crypto-evidHeader} + T_{send-evidHeader} = \\ &= T_{crypto}(Testim.Collection(REQ)) + T_{trans}(Testim.Collection(REQ)) + \\ &+ T_{crypto}(Testim.Collection(WIT)) + T_{crypto}(Evid.Generation(REQ)) + \\ &+ T_{trans}(Evid.Generation(REQ)) + T_{send-testimony} = \\ &= (14.31 + 1 \cdot 670.51) + 0.47 + (708.1 + 2 \cdot \sigma_v) + (341.59) + 0.52 + 0.26 = \\ &= 1735.76 + 2 \cdot \sigma_v ms. \qquad (8.19)\end{aligned}$$

In the previous expression, T$_{trans}$(x) refers to the transmission time shown in Table 8.8 for Algorithm x, whereas T$_{crypto}$(x) represents its cryptographic processing as shown in Table 8.6. Moreover, time T$_{send-testimony}$ has been calculated by simply isolating the transmission costs of the testimony from T$_{trans}$(Testim. Collection (WIT)). Noted that the previous calculations have considered that the testimony is referred to the position (which is slightly bigger than that referred to the speed). At the light of this result, it may be seen that this execution, under ideal conditions, takes around 1.8 seconds to be performed, plus two times σ_v, required to verify public key certificates. It should be noted that the time to verify the certificate status in the signature verification of the evidence header acknowledgement has not been considered. This decision is taken because the message issuer is the Evidence Manager, which is a well-known entity from the background environment. Therefore, it is assumed that its certificate is already verified at the beginning of this process.

Vehicular storage needs for the witness

In general words, the witness is forced to (1) perform a connection to EM using the resilient channel at a periodic basis (typically, daily) and (2) if necessary, give the pending testimonies using that connection (being called for maintenance if it is not performed). For this purpose, vehicles have to store the behavior-related data contained in the incoming beacons. This need implies that vehicles have to be equipped with a storage unit. The size of such device will affect to the suitability of this proposal to a real vehicular environment.

In order to estimate the storage needs (see Table 8.9), it is necessary to determine the amount of incoming beacons. Such amount is determined by the density of vehicles that are around a given one in its connectivity range. Given that the maximum range of the vehicular (i.e. DSRC) connection is one kilometre, it is necessary to establish the amount of vehicles in a square kilometre. In a urban environment, where vehicular densities are expected to be higher than in regular highways, such value ranges from 40 vehicles / km^2 (in a very sparse situation) to 320 vehicles / km^2 (in a highly dense one) [83]. Taking into account that beacons are sent every 100 ms. ([59]), vehicles may be receiving from 400 to 3200 beacons per second. For each one, a total amount of 18 bytes is necessary for its storage – 2

	d = 40 vehicles / km^2 (very sparse)	**d = 80 vehicles / km^2** (sparse)	**d = 160 vehicles / km^2** (moderate)	**d = 240 vehicles / km^2** (intense)	**d = 320 vehicles / km^2** (highly dense)
Beacons received per second	400	800	1600	2400	3200
Storage needed per second (bytes, considering 18 bytes per beacon)	7200	14400	28800	43200	57600
Storage needed for a one-hour trip (Mbytes)	**25,92**	**51,84**	**103,68**	**155,52**	**207,36**

Table 8.9: Witness storage needs for one-hour trip under different vehicular densities

bytes for the speed value, 10 bytes for the positional (latitude, longitude, elevation) information, 4 bytes for the vehicular identifier and 2 for the time mark [59]. This leads to the amount of storage required for one second. Generalizing this value for a one-hour trip (which seems to be reasonable for an urban environment), the maximum storage required in the worst case (i.e. higher density) is 207,36 Mb. It should be noted that the real value could be lowered if the network reliability were considered, as some data losses could happen.

Apart from this information, it is necessary to store the testimonies that have been sent in the whole period, as they may have been lost in the vehicular channel. The storage needs for each testimony is 24 bytes in the worst case (i.e. position testimonies), considering the testimony contents (recall Section 7.4.1) and data sizes (Table 8.7). However, the amount of testimonies is significantly smaller than that of beacons at stake. Considering 100 testimonies in the aforementioned trip, the required storage would be 2400 bytes.

At the light of these values, the storage needs are reasonable for the vehicular context. However, if such storage need were not suitable for the future early development of the vehicular devices, other protocol designs could be proposed. Two of them are introduced following. First, a probabilistic approach could be adopted for implementing a deletion policy in a witness. Thus, the witness will delete a given record from a previous beacon with a given probability. In this case, the proposed protocol should be changed to allow a ’unknown requester’ answer in the testimony exception handling procedure.

The second approach could be to limit the storage period of beacons to the time required to receive the request from the requester, taking into account typical values for the vehicular computational and network cost for the requester (Section 8.4.2) and t_{gap}, i.e. the time gap between the offence and the notification (Section 8.4.2). In such a case, it could happen that once the exception handling procedure is launched, the witness does not have the data to build the testimony. However, such testimony should have been created in the moment in which the request was received. The only way for an uncooperative node to avoid participating in this protocol should be to argue that it did not receive the request from the requester. However, it may be defined a maximum amount of allowable times in which such justification could be used. Particularly, using the relationship between packet delivery ratio and sender-receiver distance shown in [74], it is possible to probabilistically determine the plausibility for a given message to be lost in the network. Beyond that threshold, the Authority would call to the vehicle for maintenance in order to check up its communication devices.

Vehicular storage needs for the requester

In the time interval between the offence and the notification (t_{gap}), the requester has to store (1) its in-vehicle sensor information and (2) the set of received beacons. The first information is needed to evaluate whether the received notification is fair or not based on its perceived driving behavior. The second information is required to build the evidence header, as the beacons of purported witnesses have to be included in such structure. It should be noted that the second information is different to that required to the witness – in this case, not only the beacon sensorial data must be stored, but the whole beacon itself. The storage costs for both types of data is illustrated below. Apart from these data, the requester has to store the evidence headers that have not been acknowledged. However, it is estimated that this storage need is negligible compared to the previous ones, as it is only necessary when an evidence is to be created and only if the vehicular channel transmission is not successful.

Concerning the storage of sensorial information, it depends on four factors – the amount of sensors $nsen$, their sampling speed $samsp$, the size of the sensorial values $sval_i$ and the time mark of each sample $tmark$, and t_{gap}. Particularly, the requester storage $RqSt$ is given by Equation 8.20.

$$RqSt = \frac{t_{gap}}{samsp} \cdot (tmark + \sum_{i=0}^{nsen} sval_i) \tag{8.20}$$

For the context of this contribution, only position and speed sensors will be considered ($nsen = 2$). Concerning the sampling speed, it is desirable that it is not higher than the rate at which beacons are sent. In this way, every beacon contains fresh (i.e. not repeated) sensorial data. For these calculations, the value $samsp = 100\ ms.$ will be taken, which coincides with the beaconing rate assumed in current standards. The size of the sensorial value is 2 bytes for the speed value ($sval_0$) and 10 bytes for the positional information ($sval_1$). The time mark size $tmark$ is 2 bytes [59]. Concerning the interval t_{gap}, the values 5, 30, 60, 180 and 300 seconds will be considered. At the light of these values, it may be seen that in the most favourable case ($t_{gap} = 5$) $RqSt = 700\ bytes$ while in the worst case ($t_{gap} = 300$) $RqSt = 42000\ bytes$.

With respect to the storage of received beacons, the calculation follows an analogous reasoning as that presented in the previous subsection. The difference is that in this case it is necessary to store the whole beacon, but only during the period t_{gap}. According to standard SAE J2735, the beacon data size without considering optional parts is 49 bytes (recall Figure 5.1) [59]. As it is assumed to be signed, the public key certificate and digital signature (125 and 56 bytes respectively, ac-

	d = 40 vehicles / km^2 (very sparse)	**d = 80 vehicles / km^2** (sparse)	**d = 160 vehicles / km^2** (moderate)	**d = 240 vehicles / km^2** (intense)	**d = 320 vehicles / km^2** (highly dense)
Beacons received per second	400	800	1600	2400	3200
Storage needed per second (bytes, considering 230 bytes per beacon)	92000	184000	368000	552000	736000
Storage (Mbytes) needed for t_{gap} = 5 s (best case)	**0,46**	**0,92**	**1,84**	**2,76**	**3,68**
Storage (Mbytes) needed for t_{gap} = 300 s (worst case)	**27,6**	**55,2**	**110,4**	**165,6**	**220,8**

Table 8.10: Requester storage needs for beacons considering $t_{gap} = 5$ s. (best case) and $t_{gap} = 300$ s. (worst case) scenarios

cording to IEEE 1609.2 [8]) must also be considered. Thus, each beacon requires 230 bytes of storage. Considering this value and the previous ones for t_{gap}, Table 8.10 summarizes the results for the storage needs in different scenarios. It may be seen that in the less favourable context (i.e. the highest vehicular density and the greater time interval between offence and notification), the requester has to store 220,8 Mb.

Experimental evaluation

In order to assess the amount of evidences and testimonies per evidence that may be achieved in a road scenario, several simulations have been conducted using the NS-2 simulator. This evaluation will focus on the viability of the proposed protocol assuming that the computational devices have enough resources to perform the required computation. Thus, there are no bottlenecks caused by the inherent existence of several time-consuming tasks, such as beaconing signatures or safety-related ITS services. In the same way, delays introduced by other underlying procedures (such as public key certificate updates, plausibility checks over the received information, certificate revocation list downloading, etc.) are not considered in these experiments.

The main simulation parameters are shown in Table 8.11. The transmission parameters are derived from the expected performance of DSRC communications including their data rate, reception range and channel reliability [81]. With respect to the routing strategy, in this evaluation the use of a one-hop broadcast has been chosen. As this is the most basic dissemination strategy (as there is no forwarding between nodes), it avoids introducing delays caused by a routing strategy, as well as routing errors. It should be noted that routing in these networks is a matter of open research, so the election of a given strategy could have a great impact over the results [71]. For the purpose of this evaluation, it will be assumed that all vehicles are equipped with non-compromised vehicular platforms.

In order to assess the suitability of the proposal to the changing reality of vehicular situations, five representative scenarios have been considered, namely a urban section from the city of Eichstätt, a highway stretch, a highway crossing section, a secondary road and a Manhattan-like map. In each one, 250 vehicles have been simulated over 600 seconds.

The vehicle movement has been created using both SUMO [84] and CityMob [85] mobility traces generators. Particularly, the considered vehicular speeds are up to 10 km/h higher than the current speed limit. From our point of view, this situation adequately reflects the current driving practices. It should be noted that this decision leaves out those vehicles that are significantly speeding. This fact is irrelevant for the vehicle that is requesting for testimonies because, if it was really speeding, the fine notification would be considered as fair and therefore the whole evidence generation process would not be started. However, this could have an impact over the reachability of witnesses – if they were actually speeding whereas the requester were not, they could get out of range in a shorter time. From our point of view, this decision should not have a significant impact on the evaluation

Parameter	Value
Data rate	6 Mb
Reception threshold	300 m
Wireless frequency	5.9 Ghz
Routing protocol	None (broadcast)

Table 8.11: Simulation parameters

results, because (1) the proportion of speeders is usually not very high, and (2) it is not likely that a vehicle which is committing an illegal action would be willing to participate as a witness. Nevertheless, an extended evaluation taking into account this issue is left to future work.

An intuitive assumption is that the smaller t_{gap} is, the closer (consequently, the more reachable) the Witness may be from the Requester. Therefore, this analysis will be focused on determining the effect of t_{gap} in (1) the proportion of valid witnesses that are reachable and (2) the amount of testimonies that will be sent for each offence. The first indicator shows the relationship between the *potential* witnesses and the *actual* witnesses, whereas the second one shows the total amount of *actual* witnesses. In this way, it is possible to characterize both the achieved and missed testimonies.

Figure 8.6 shows the ratio of available witnesses in each scenario, using 5, 30, 60, 180 and 300 seconds for t_{gap}. Except from the highway, around 90 % of the witnesses are available if $t_{gap} = 5$ s. On the contrary, for $t_{gap} = 300$ seconds this proportion drops below 30 %. For the intermediate value of $t_{gap} = 60$ seconds, all scenarios except the Manhattan map allow for a proportion of around 50 %. There are two facts that should be analysed separately. First, the highway scenario never offers a ratio higher than 52 %. This is due to the high speed of vehicles, along with their potential greater speed differences, making it more probable to get out of range very soon. Second, the ratio offered by the Manhattan map gets lower faster than the remaining ones, significantly before $t_{gap} = 30$ seconds. This fact is a consequence of the map definition – once a vehicle turns in a street, it starts

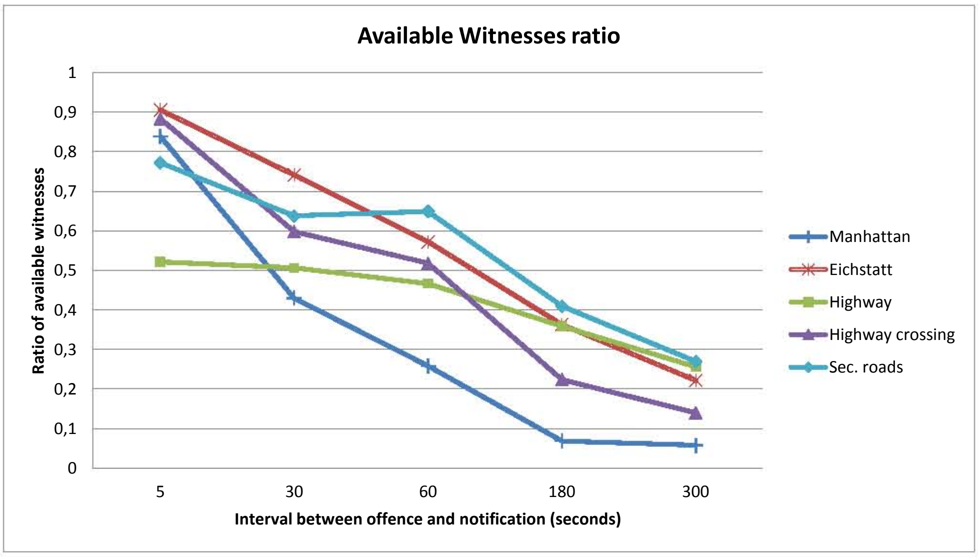


Figure 8.6: Ratio of available witnesses for different t_{gap} values

driving in a perpendicular direction to the other one.

On the other hand, Figure 8.7 shows the amount of available testimonies in each scenario for the aforementioned values of t_{gap}. The highway scenario is the most convenient one, as it offers the maximum amount of testimonies for all values of t_{gap}. Remarkably, 38 testimonies are collected for $t_{gap} = 5s$. This may be explained by the multi-lane feature of such kind of roads, which enables more vehicles to be in range. On the contrary, the Manhattan map is the one that offers the lower amount. This fact may be due to the fast dispersion of vehicles in this map according to the considered mobility pattern. Although the amount of required testimonies to endorse a given claim is up to the Adjudicator, we assume that having less than 10 testimonies may be inconvenient. Based on such assumption, this protocol may be used in highways for every t_{gap}, whereas in secondary roads it is not suitable for t_{gap} = 300 s. In the Eichstätt and highway crossing settings, it is only suitable for $t_{gap} \leqslant 180$ seconds. The proposed protocol is not suitable for the Manhattan map under this criterion.

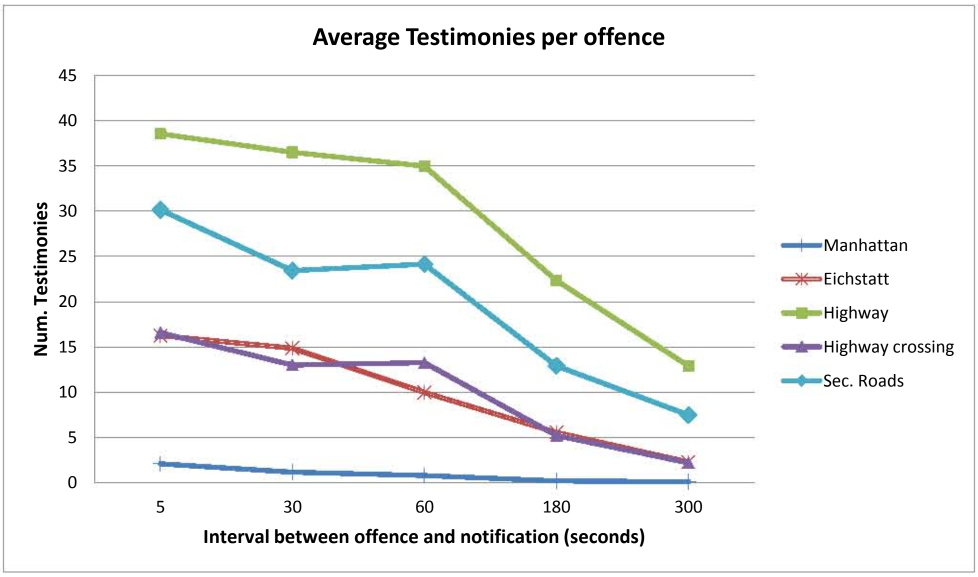


Figure 8.7: Average amount of testimonies per offence for different t$_{gap}$ values

8.4.3 Security requirements analysis

This Section evaluates whether the imposed requirements are fulfilled and, consequently, if all threats have been countermeasured. Table 8.12 summarizes the analysis presented herein, capturing the countermeasures adopted against each threat for every message. In such table, apart from the data structures introduced in Section 7.4.1, the evidence header acknowledgement is also considered because of its relevance in the process.

Correctness. The Evidence verification algorithm enforces that the evidence contains at least one supporting testimony (condition 1). In this way, evidences based on false claims by R are removed, as there would be no supporting testimonies. Moreover, the semantic checks ensure the consistency between at least one of the testimonies and R's claimed value (condition 2). The time consistency (condition 3) is also checked in the verification process. It must be recalled that this verification is possible since vehicles are assumed to be synchronized by means of the integrated navigation system. The verification process also checks that all pseudonyms at stake belong to a different entity (condition 4), and that the W$_i$ identified by R (i.e. listed in the evidence header) is the one that generates one of the supporting testimony (condition 5).

Concerning the threat of messages never created or lost, the use of a resilient channel (once the vehicular one has failed) contributes to mitigate it for all messages except from requests (see Table 8.12). In such case, the Testimony exception handling enables collecting the testimony even if the request was not received by the witness. Therefore, even if the request is lost, the correctness is not threatened.

With respect to the message alteration, the use of digital signatures (which have been created in a secure environment) makes it possible to detect this threat. The same mechanism avoids the chance of impersonation, which may be seen as an alteration of a legitimate message.

Confidentiality. All messages exchanged in the vehicular environment are encrypted to its intended receiver – the request (encrypted to each W_i), the testimony and the evidence header (to the EM). Moreover, the created evidence is sent encrypted to Adj. Moreover, these data are securely managed by their respective receivers (SAE_{Wi}, EM and Adj, respectively).

Authentic requests. The contents of the request ensure that R is the same entity to which the evidence has to be referred, as it has one part digitally signed under such identity ($R(t_{off})$). Moreover, another part is signed under its current identity ($R(t_{req})$), which prevents third parties to issue requests referred to others. The time mark t_{off} introduced in the first part counters the potential threat posed by replay attacks.

Authentic testimonies. The verification process checks the plausibility of a given testimony. In this way, sensor errors (accidental or on purpose) are properly handled if such checks offer a reasonable reliability. Therefore, the proposed approach satisfies this condition to the same extent as real-life Court situations – witnesses may be good-willing but they may offer wrong testimonies as a result of their perception errors.

Message	**Threat**	**Countermeasure**
Request	Not created / Lost	Testimony exception handling process over an operational channel (this countermeasure solves the *consequences* of this circumstance, but not this issue itself).
	Altered / Created by unauthorized party	Digital signatures (using the private keys related to R(t$_{req}$) and R(t$_{off}$)) using a secure device (HSM) in a trusted environment (OVERSEE). Supported by a secure build-up management process. Message verification operations performed by the witness.
	False data (e.g. unrelated to an ongoing offence)	Out of the scope (irrational attack).
	Eavesdropping	Encryption using every witness' public key.
Testimony	Not created/ Lost	Testimony exception handling process over an operational channel.
	Altered / Created by unauthorized party	Digital signature using a secure device (HSM) in a trusted environment (OVERSEE). Supported by a secure build-up management process.
	False data (sensor failure or malicious manipulation)	Plausibility checks.
	False data (non-present witness)	Secure Location Verification service.
	Eavesdropping	Encryption using EM's public key.
Evidence header	Not created	Out of the scope (irrational attack).
	Lost	Evidence header exception handling process over a resilient channel.
	Altered / Created by unauthorized party	Digital signature using a secure device (HSM) in a trusted environment (OVERSEE). Supported by a secure build-up management process.
	False data (modified witness list)	Neighbour list is managed in the trusted environment (SAE). Digital signatures may only be performed in genuine HSM (secure build-up management process) and only upon request from the SAE (trusted environment). Therefore, it is not possible to create a well-formed message with an invalid neighbour list.
	False data (unrealistic claim)	Evidence verification will discover no supporting testimonies, so the evidence will be discarded.
Evid. header ack	Lost	Evidence header exception handling process over an operational channel.
	Altered / Created by unauthorized party	Digital signature in a trusted environment.
	Not created / False data	Not possible (EM is trusted).
Evidence	Lost	Sent by a trusted entity (EM) through a resilient network, to the Adjudicator.
	Altered / Created by unauthorized party	Digital signature in a trusted environment.
	Not created / False data	Not possible: EM is trusted and plausibility checks are conducted to verify the data.
	Eavesdropping	Encryption using Adj public key.

Table 8.12: Requirements and threats evaluation for each data structure

Moreover, the Secure Location Verification process, along with the beacons contained in the evidence header, ensure that the witness was present when the offence was committed. As the cryptographic material is securely loaded into the HSM, and given that such device is firmly attached to the vehicle, only such vehicle (which is necessarily different to R) is able to correctly sign a message. As testimonies are digitally signed, there is no chance for impersonating the witness.

8.5 Comparison of the contributions against previous works

8.5.1 Analysis of the proposed model

The improvement of the road traffic enforcement process has received several contributions. Most of them are the result of European research projects.

The ESCAPE project analyzed the process at an European level and identified its effects, measures, needs and future [4]. The enforcement weaknesses pointed out by this project, as well as its suggestions to introduce new technologies on this field, is a starting point for the work developed in this thesis.

The FAIR (Fully Automatic Integrated Road control) project aimed to improve the enforcement by using different surveillance technologies along the roads [86]. Achieving an immediate feedback for the offender (which, in the end, is the intended consequence of the goal O3 of this thesis) was pointed out by FAIR as a future research issue.

The efficiency and effectiveness of the enforcement process was the focus of the PEPPER (Police Enforcement Policy and Programmes on European Roads) project [87]. This project pointed out that ITSs could improve the enforcement process, although there were several legal, technical, and operative issues that should be addressed first. One of the goals of this thesis (goal O1) is to design a model that helps on understanding this process, clarifying how ITS technologies may be integrated in this context.

Finally, the European architecture on ITS (already introduced in Section 3.5) provides support for the enforcement process, particularly for the Starting phase [48]. Even if it introduces interactions with the vehicle to get some data, the problems considered in this thesis (see Section 3.4) are not addressed in the current version of this architecture.

8.5.2 Analysis of the proposed covert reporting mechanism

To the best of the knowledge of this thesis' author, there are no previous contributions on applying steganography in the vehicular context. However, in order to determine the novelty of this contribution, it is necessary to analyze other previous works that are related in some way to the proposal.

As compared to the watermarking schemes proposed by Fang et al. [32] and Zhang et al. [33], the contribution presented in this thesis tries to achieve a different goal. In their case, modifications to sensor data are performed to authenticate them. In the proposed approach, the modifications are introduced with a totally different purpose (reporting a misbehaving vehicle) which is not related to the sensorial data at stake.

Concerning the scheme of Sion et al. [34], the contribution presented herein is similar in that both have a common definition of usability for a given value. Sion et al. defined an *usability metrics*, whereas in the presented contribution there is a reliability interval that establishes the maximum amount of data that may be embedded into a given data field.

8.5.3 Analysis of the proposed notification protocol

In the context of vehicular networks, there are several ITS applications that have two points in common with the notification process described so far – (1) that the message arrives to the vehicle and (2) that it is possible to attest this issue for an eventual dispute resolution process. Two representative examples of these applications are introduced below.

First, the electronic signage (i.e. the electronic transmission of traffic signs to the vehicle) has been identified as a beneficial application, especially for old drivers [88]. In a future scenario in which the traffic signs were transmitted exclusively in this way, it could be necessary to ensure that the vehicle received this information in order to punish offenders.

Second, the Enhanced Driver Awareness (EDA) application enables the driver to receive sensorial data from other vehicles and infrastructure elements [89]. Again, if the driver takes a decision which leads to a traffic incident, and if it is against the data received through EDA, the liability attribution could be more severe than that of an unexpected incident.

Despite the prior description, and to the best of the author of this thesis' knowledge, none of these applications have addressed the scenarios in which the message does not arrive to the receiver or there is no proof on the correct reception by the vehicle. The contribution presented in this thesis takes both issues into account by (1) establishing a retransmission scheme that fights against the unreliability of the vehicular channel and (2) using a trusted third party over a reliable connection for the cases in which the vehicular network is not enough. However, it should be noted that the use of such reliable connection occurs after a significant time interval. As opposed to what happens with the notification, such interval would not be suitable for the aforementioned applications. Thus, sending a traffic sign that was in force for a previous road stretch would be useless, as well as receiving EDA information that applies to a former traffic scenario.

8.5.4 Analysis of the proposed cooperative evidence generation protocol

The small amount of contributions related to evidence generation in vehicular scenarios were already introduced in Section 3.3.3. In this Section, each of these contributions is confronted with the one presented in this thesis.

First, compared to [43], it should be noted that the contribution developed in this thesis takes into account not only the own vehicle's sensor measurements, but also data coming from the surrounding vehicles. Taking into account that it would now be required for an attacker to compromise (or to collude) the surrounding vehicles, the chance of such attack is lower than that of the proposal in [43].

Second, in comparison with the security framework presented by Lin *et al.* [44], they consider as an evidence a signed message sent by a given vehicle, using ID-based cryptography and group signatures as the underlying cryptographic mechanisms. In the contribution presented in this thesis, the evidence is the result of signing a given (also signed) claim by the requesting vehicle, along with a set of supporting (signed as well) testimonies. Furthermore, the cryptographic approach is based on public key cryptography according to the IEEE 1609.2 standard.

Finally, group communications could be envisioned as a means to select witnesses. Group formation has been previously studied by Raya *et al.* [90]. Nevertheless, the requesting vehicle in the contribution presented in this thesis is requiring information of a moment in the past. Given the volatility of the group formation, it could be possible that current group members were not present at the requested time. For this reason, in this work the use of group communications have been discarded, as this choice would not always be suitable.

Chapter 9

Conclusions

This Chapter contains the thesis conclusions and final remarks, and summarizes the contributions achieved. A critical discussion on the developed work is also presented. Additionally, future research directions that derive from the thesis results are proposed.

9.1 Conclusions and summary of contributions

The work developed in this thesis has been focused on the improvement of the road traffic enforcement process. Such process is critical to ensure that every offence is rapidly reported by the Authority. In this way, drivers feel that the probability of being caught is high, thus forcing them to drive more responsibly.

Despite the relevance of the enforcement process, current implementations suffer from a high bureaucracy and a low degree of participation of regular citizens. In order to contribute on these issues, this thesis has focused on creating new mechanisms of communication between the Authority, the offender and the potential victims or witnesses. For this purpose, a new technological trend called Intelligent Transportation Systems (ITS) has been considered. ITS consist on the application of Information and Communication Technologies (ICT) on the vehicular environment, thus enabling vehicles to communicate among them in a real-time fashion. The main conclusion of the work developed in this thesis is that the use of ITS technologies is an interesting approach to contribute on improving the enforcement process.

Prior to creating any mechanism, it is necessary to have a comprehensive model that clarifies the participant entities and their relationships. The first contribution of this thesis has been to develop such model (see Chapter 4) for speeding offences based on the results of a related European project called VERA2. Thanks to this model, the phases, the data at stake, the data exchanges and the underlying security considerations have been described. With such a clear vision on the process, the integration of ITS technologies in this context is clarified.

Based on the aforementioned model, three mechanisms have been proposed for different steps within the process phases. The first one (see Chapter 5) is related to the automatic reporting of an offending vehicle by its surrounding vehicles. In this way, detecting offences is not a task almost exclusive for the Authority, but instead any citizen is able (in a practical way) to report their occurrence. To avoid the potential retaliation by the offender to the reporter, the use of steganography has been proposed to secretly embed the report within regular ITS-related messages. Particularly, the most frequent message structure, called *beacon*, has been selected as the carrier for such reports.

Once a traffic offence has been detected, the second mechanism is intended to improve the immediacy on the notification step, that is, to formally inform the offender on the legal consideration of the committed fault. The proposed notification mechanism (described in Chapter 6) enables delivering the message to the offending vehicle while keeping the legal provisions related to its validity. Furthermore, under the assumption that the vehicle will force the driver to take a decision on the notification (the next time he/she attempts to use the car, at the latest), the chance for ignoring the notification (i.e. the so-called *passive behavior*) is countered.

The third and last mechanism is related to those undesirable situations in which the reported driver finds that the received fine is not fair. This is the case when, for example, a speeding offence is reported while the driver claims that it was not speeding. Similarly, it may happen that the reported speed is higher than that claimed by the driver, leading to a more severe punishment than that expected by the driver. In fact, this could be the result of an inaccurate report created using the first mechanism proposed. Such third mechanism (see Chapter 7) enables the reported driver to gather the viewpoints from surrounding vehicles, using them as witnesses. In this way, it is possible to obtain a more complete vision of the facts, leading to a more fair enforcement system.

Globally, the aforementioned contributions enable a more active participation of all citizen stakeholders of an enforcement process – the offender, the potential victims and the surrounding witnesses. Such contributions have been shown to be feasible under realistic assumptions over computation devices, communication networks and road traffic scenarios.

The aforementioned contributions have been published in several papers. Annex B shows the list of publications. The relationship between each contribution (using the numbers given in the aforementioned Annex) and the corresponding publications is shown in Table 9.1. It should be noted that publications 4, 5 and 7 are not related to any contribution in particular, but instead they are previous works that served as a basis to develop these contributions.

Contributions	**Publications**
C1. Complete enforcement process model	1, 6, 8
C2. Steganography-based protocol for covert reporting of misbehaving vehicles	9
C3. Protocol to send an offence notification to the offending vehicle	10
C4. EVIGEN protocol for cooperative evidence generation	2, 3

Table 9.1: Relationship between contributions and publications

9.2 Critical analysis on the developed work

The work developed in this thesis is focused on improving different aspects of the enforcement process. Even if the existence of problems in such process was already detected by previous European projects, there are not indicators on the size of these problems in a practical system such as the Spanish enforcement one. Therefore, there are not figures on the amount of voluntary reports created by citizens, so it will be not possible to determine the degree of improvement achieved by the inter-vehicle reporting protocol. Concerning the notification protocol, it enables a fast delivery of such message. However, there are not official measurements (only rough estimations) on the current delay of the notification step, making it impossible to determine the benefits of the proposed mechanism. Related to this point, having a faster notification mechanism may help on decreasing the number of reports that expire. However, it is unknown (at least, not publicly available) the current amount of reports that expire before they have been processed. Similarly, there are not indicators on the amount of evidences presented by citizens, which makes difficult to measure the benefits of the evidence generation protocol.

As an addition to the previous point, the lack of implementation in a real system of the proposed mechanisms makes it difficult to estimate their impact in a real-world environment and, particularly, their potential misuses. Concerning the inter-vehicle reporting mechanism, it should be noted that it could be used maliciously – for example, a given vehicle may falsely report others just to make harm. Similarly, the evidence generation protocol could be used to create false testimonies by coalitions of drivers. In both situations, it is necessary to develop a trustworthiness analysis procedure, which has been identified in this thesis but left to future work. Even if the work developed in this thesis enables the implementation of the proposed mechanisms, having such analysis procedures is a prerequisite for the practical use of the developed contributions. It should be noted that the evidence generation may serve as a conceptual deterrent for such a lack of trustworthiness in reports. Thus, in case that a false report is issued, the set of testimonies supporting the reported driver's argument will serve to lower the reliability of the aforementioned report.

The aforementioned lack of real implementation also affects to the accuracy of the evaluation conducted on this thesis. In general terms, the evaluation is almost fully theoretical. In order to obtain experimental measurements, simulators (or performance figures of commercial vehicular devices) have been used. Although the employed simulator (NS-2) is well-known, the realism of the created mobility trace has a direct impact on the applicability of the results to a real-world environment. Therefore, even if it is a widespread way of validation for ITS-related proposals, the evaluation should be extended to confirm the suitability of the proposed mechanisms. Furthermore, it should be confirmed that the impact of speeding vehicles (especially in the evidence generation protocol) is not significant for the evaluation results.

Regarding to the evaluation settings, there are two issues that should be revised. First, the processing capabilities of Road Side Units (RSUs) have been assumed to be enough to perform the required operations. However, this issue should be contrasted with practical devices. Second, it should be measured the performance of the proposed mechanisms in more complex vehicular scenarios where several ITS services are coexistent. Additionally, it should be taken into account the potential impact of different routing protocols (AODV, geocasting, etc.) or even addressing techniques (WAVE Short Messages Protocol, IPv6, etc.). Specifically for the proposed evidence generation protocol, the analysis has been based on ideal conditions where there was no other workload different from that of the studied protocol. Such analysis should be extended to ensure that it is suitable even in a real vehicular scenario where several applications are running at the same time.

Most of the considered legislation which forms the legal basis of this work is the Spanish one. Although the underlying principles should be very similar to other countries, this election may have caused that the developed mechanisms are only fully applicable (in their current form) in Spain. Nevertheless, it should be noted that the VERA2 model that served as a basis for the proposed model was already defined in the European context, and only a small amount of refinements was required to adapt it to the Spanish current legislation.

Concerning the application of steganography in this context (for the inter-vehicle reporting mechanism), there are not unique, well-known analysis on the degree of randomness of the in-vehicle sensor measurements error. In its current form, the proposed mechanism assumes that such error is fully random. This situation is the most convenient one (from the steganographic point of view), as it enables the maximum capacity for each sensor data field (according to the definition of capacity shown in Chapter 5). However, it is necessary to perform an experimental validation of this issue in order to determine the actual capacity of these fields.

As an addition to the previous point, the use of steganography by altering the sensorial data in beacon messages may be seen as unacceptable by road traffic safety experts. It must be noted that these messages are defined to help the driver to have a wide vision on the road traffic status. Thus, introducing errors (even smaller) in such messages may be seen as an unnecessary source of uncertainty, which may lead to a low acceptance by manufacturers or even governments.

One issue related to all the mechanisms proposed in this thesis is that they have been developed without the supervision or guidance of the National Traffic Authority (Spanish DGT). In this way, it is not possible to determine whether the proposal fits within the practical realizations of the enforcement system, or even if they are suitable to the vision of such Authority on the road traffic safety mechanisms. It must be noted that the implementation of the proposed mechanisms may require additional investments, which may be not well-accepted taking into account those already performed in this issue (e.g. ESTRADA processing station, the use of PDAs by policemen, etc.)

Last but not least, the use of Hardware Security Modules (HSMs) has been adopted as a root of trust throughout this thesis. This assumption, which is also shared by other research initiatives such as the OVERSEE European research project, is beneficial in that it constitutes a basis over which the remaining security mechanisms may be built. However, achieving such level of reliability in a single physical device constitutes a technical challenge. Therefore, it is interesting to discuss the impact on the proposed mechanisms of decreasing the assumed reliability of HSMs.

Related to the reporting protocol, the lack of a secure key storage would enable that the reporting device could impersonate others. This scenario could make such reports impractical – in case that a given report is said to be false, there would be no reliable way to reveal the identity of the real reporter.

Concerning the notification protocol, without such a trusted component there would be no way of ensuring that notifications will be delivered to the vehicle *only* when their receiving person is able to gather them. Furthermore, the time in which the notification is received or accessed could be forged, which may be of interest for a driver, trying to delay as much as possible the starting time of the legal period for building counterevidences and allegations. Apart from the previous points, the lack of secure management of the private keys would enable to transfer (or copy) them to other vehicles, which could impersonate the former. In this case, it is important to note that it would threat the confidentiality of the notification message.

With respect to the evidence generation protocol, the aforementioned lack of secure storage would lead to an undesirable scenario in which a single vehicle could (1) self-generate as much testimonies as it wishes, using identities obtained from other vehicles, (2) hand-craft the list of available neighbours, thus forming groups of preferred witnesses which are even not in the surroundings, (3) act as witness on behalf of a third vehicle.

9.3 Challenges and future research lines

The work developed in this thesis opens the door to several innovative research lines (with their associated challenges), which are mainly focused on complementing the approach or even extending it to other related areas.

Concerning the model proposed, the first challenge is to generalize it in order to be suitable for other kinds of enforcement processes (different from the administrative one covered in this work) and for other traffic offences (different from the speeding one). The goal is to make it suitable across Europe, but it requires to identify the common issues (and also different) among different countries.

On the other hand, due to the practical application of the mechanisms described, the challenge is to implement them in a real environment. For this purpose, the collaboration of the Spanish Traffic Authority is critical, as it is the entity that would be managing the resulting system. The practical challenge resides on the adaptation of current systems (mainly, the ESTRADA processing station) to the expected workload that would be derived from the proposed mechanisms. The resulting time gap between the offence and notification should be carefully analysed in order to quantify the level of improvement. At the same time, the degree of impact in the driver's attitude should also be studied.

Additionally to the previous point, it is also critical to research on the best way of presenting the message to the driver. Such procedure should fulfil two (potentially opposed) goals, namely to ensure the maximum educational effect of the punishment (which usually requires raising a significant level of awareness) without interfering in the driving task (thus avoiding distractions).

Continuing with the improvement of existing practices, it is interesting to analyse if the offender identification can also be improved by means of ITS-related technologies. Current offences detected by automatic devices are firstly referred to the vehicle keeper because there is no way to reliably identify the offending driver. However, as an extension to other research projects (e.g. Spanish PRECIOUS, undertaken by the Security on information technologies research group of the University Carlos III of Madrid), the existence of an Electronic Driving License could allow performing an electronic authentication of the actual driver. Notwithstanding, the privacy protection of such person must be ensured, especially avoiding the risk of tracking (i.e. determining the path followed by a given person). For this purpose, it is critical to analyse the specifications on this issue made by recent standards, specially ISO 10711:2012 [91].

Concerning new alternatives for the proposed approach, it is worth to consider the growing amount of connected mobile devices. They may be connected to the in-vehicle network and, at the same time, to other devices either through short range technologies (e.g. Bluetooth) or long range ones (e.g. satellite communications). Even if they cannot be used while driving, they may act as a substitute of OBUs. Moreover, cryptographic capabilities introduced in some SIM cards make them more interesting as an active part of data exchange protocols that require such kind of operations (as those proposed in this thesis).

There are three main ways in which the approach presented herein may be extended. First, the steganography-based reporting mechanism could be adapted to enable cooperative reports. In such a new scenario, several vehicles could covertly share their vision about a third (suspicious) one. If they agree on that it is a offender, they may create a combined report. In this way, offences that involve a set of dangerous actions could also be detected. It must be noted that the severity of an offence that comprises a group of actions is sometimes greater than the mere sum of that of these actions. For example, reckless driving is a severe offence which is usually composed by a set of dangerous actions that have been committed over different victims. Similarly, this mechanism could be extended to cope with continuous infractions. Thus, a speeding offence committed over a stretch of 5 kilometres should receive a higher punishment than that performed at a single moment. Second, the impact of cross-border enforcement over the proposed mechanisms should be studied. The extent of validity of reports made by a citizen from a country in a foreign one remains as an open issue. At the same time, presenting a notification message in the driver's native tongue, even if she is driving in a foreign country, may be achieved by different ways. Third, the non-repudiation needs detected for the notification mechanism are, at least in theory, similar to those ITS services where liability attribution may arise. This is the case of in-vehicle signing (i.e. sending electronically road traffic signs directly to the vehicle). It is necessary to clarify the extent of this need (particularly on the consequences of a failed delivery of such messages) and introduce the appropriate mechanisms to address it.

In the notification protocol it has been assumed that it is possible to determine the set of potential locations in which a vehicle may be some time after the offence has been detected. Such estimation requires an in-depth analysis of the vehicular movement and traffic conditions, in order to calculate the minimum set of locations (to avoid overloading more RSUs than strictly necessary) without loss of effectiveness (to ensure that the receiving vehicle is in one of those locations).

Related to both the reporting and notification mechanisms, the use of a simple repetition scheme has been selected as a means to promote the correct transmission of the messages at stake through the vehicular (unreliable) channel. Thus, the use of existing error correction codes (recall Section 5.6.1) or the potential development of other equivalent mechanisms that are suitable for this context is a matter of future research. Such mechanism must face the fact that the message may be received by not only one entity (i.e. a single RSU) but by a set of independent entities, as it was explained in the reporting protocol. This issue should be taken into account as it enables re-sending a given message or its error correction codes. This could simplify the complexity of the required operations to calculate the code, as the error rate could be lowered by this re-sending operation.

On the other hand, the threat of collusion has been left out of the scope of the evidence generation protocol. Such a threat affects to the data trustworthiness.

Developing an evaluation procedure for this issue is a matter of future research, considering the particular conditions of vehicular mobility and the reliability of data provided by sensors. Such trustworthiness analysis will serve to expand both the proposed reporting mechanism and the evidence generation protocol.

Finally, the proposed mechanisms have been defined taking into account the high-level features of the VANET communication technology (i.e. DSRC). Despite that this technology is suffering a great evolution, it is expected that such features will not be changing significantly. Therefore, the evaluation of the performance and robustness of the proposed mechanisms is expected to be valid. Nevertheless, a future research issue is focused on analysing the impact of low-level decisions that are currently evolving, such as channel access control techniques or specific packet formats.

Part V

Bibliography and appendices

Bibliography

[1] OECD. OECD E-Government Studies. The E-Government Imperative. http://www.oecd.org/bookshop; 2003.

[2] European Parliament. European Parliament legislative resolution of 23 April 2009 on the proposal for a directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes. vol.. 184.p.338–352.

[3] Ribagorda, A. Glosario de Términos de seguridad de las T.I. Ediciones CODA; 1997.

[4] Mäkinen, T. , Zaidel, D. *et al.* Traffic enforcement in Europe: effects, measures, needs and future. Final report. ESCAPE project; 2003.

[5] Spanish Government. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. In: Spanish National Bulletin; 2007. (in Spanish).

[6] Spanish Government. Ley 18-2009, de 23 de noviembre, por la que se modifica el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 339-1990, de 2 de marzo, en materia sancionadora. In: Spanish National Bulletin (BOE); 2009. (in Spanish).

[7] Wolf, M. Security engineering for vehicular IT systems. Viewer+Teubner; 2009.

[8] Intelligent Transportation Systems Committee. IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages; 2006.

[9] European Commission. Respecting the Rules. Better Road Safety Enforcement in the European Union. A consultation paper; 2006.

[10] VERA2 (Video Enforcement for Road Authorities 2) project. Deliverable D3-1. Common Data Exchange Format and Demonstrator; 2004.

[11] La Crónica de León. La rapidez del centro ESTRADA causa las protestas de los quitamultas. La Crónica de León. 2009;.

[12] Pfeiffer, M. and Hautzinger, H. Objektive und subjektiv wahrgenommene Sanktionswahrscheinlichkeit und ihre Auswirkungen auf das Unfallgeschehen. Schlussbericht zum Forschungsproject FE 82 002-1997 der Bundesanstalt fuer Strassenwesen; 2000.

[13] Rothengatter, T. Automatic policing and information systems. Proc. of the International Road Safety Symposium; 1991.

[14] Antonio Martín. El centro Estrada pone en marcha la notificación de multas a través del correo electrónico. Dicytcom. 2009;.

[15] Juanma Lopez - Guillen G. Tráfico sólo anula el 15 por ciento de las multas recurridas. 20 minutos. 2008;.

[16] Rodriguez, J. I. Más dureza, menos accidentes. Tráfico y Seguridad Vial. 2008;.

[17] Lo, N. , and Tsai, H. Illusion attack on VANET applications - A message plausibility problem. In: Proc. IEEE Globecom Workshops.p.1–8.

[18] Dotzer, F. and Fischer, L. and Magiera, P. VARS: a vehicle ad-hoc network reputation system. In: World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium.p.454 – 456.

[19] Young, C-P. et al. Cooperative Collision Warning Based Highway Vehicle Accident Reconstruction. In: International Conference on Intelligent Systems Design and Applications, ISDA '08.p.561 –565.

[20] CAR-2-X Communication in Europe. In: Vehicular Networks: From theory to practice. CRC press; 2008. .

[21] Kargl, F. and Papadimitratos, P. and Buttyan, L. and Muter, M. and Schoch, E. and Wiedersheim, B. and Ta-Vinh Thong and Calandriello, G. and Held, A. and Kung, A. and Hubaux, J. -P. Secure vehicular communication systems: implementation, performance, and research challenges. Communications Magazine, IEEE. 2008 november;46(11):110 –118.

[22] IEEE. Standard for Motor Vehicle Event Data Recorders (MVEDRs). IEEE Std 1616-2004. 2005;.

[23] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation. IEEE Std 1609 4:2006. 2006;.

[24] Cankaya, H. , Grepet, C. , Groll, A. , Holle, J. , Wolf, M. Towards A Shared Digital Communication Platform for Vehicles. In: 18th ITS World Congress; 2011. .

[25] Gerlach, M. VaNeSe - An approach to VANET security. In: Proceedings of the V2VCOM conference; 2005. .

[26] Aijaz, A. and Bochow, B. and Dötzer, F. and Festag, A. and Gerlach, M. and Kroh, R. and Leinmuller, T. Attacks on inter vehicle communication systems-an analysis. In: Proceedings of the 3nd International Workshop on Intelligent Transportation. Citeseer;. .

[27] Provos, N. and Honeyman, P. Hide and seek: an introduction to steganography. Security Privacy, IEEE. 2003 may-june;1(3):32 – 44.

[28] Johnson, N. F. and Jajodia, S. Exploring steganography: Seeing the unseen. IEEE computer. 1998;31(2):26–34.

[29] Simmons, G. J. The prisoners' problem and the subliminal channel. In: Proceedings of Crypto 83: Advances in Cryptology. Springer-Verlag.p.51–67.

[30] Cox, I. J. et al. Digital watermarking and steganography. Morgan Kaufmann; 2008.

[31] Cachin, C. An information-theoretic model for steganography. In: Information Hiding. Springer.p.306–318.

[32] Fang, J. and Potkonjak, M. Real-time watermarking techniques for sensor networks. vol.. 5020 of Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series.p.391–402.

[33] Zhang, W. and Liu, Y. et al. Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. Pervasive and Mobile Computing. 2008;4(5):658 – 680.

[34] Sion, R. and Atallah, M. and Prabhakar, S. Digital Watermarking. vol.. 2613 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg.p.1–15.

[35] Ley 30/92, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. In: Spanish National Bulletin (BOE); 1992. (in Spanish).

[36] Toriello, A. Nuevos conceptos en la gestión de denuncias del tráfico: El centro de tratamiento de denuncias automatizadas. In: IX Spanish ITS Congress. Available online at: http://www.worlditsdirectory.com/;. (in Spanish).

[37] Chevreuil, M. Development of Automated Traffic Enforcement Systems in France. Available online at: http://road-network-operations.piarc.org/; 2005.

[38] SUPREME project. Best practices in road safety - Handbook for measures at the country level. European Commission; 2010.

[39] Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. In: Spanish National Bulletin (BOE). 278.p.97921–97949. (in Spanish).

[40] Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artculo 38.2 del Real Decreto 1671/2009, de 6 de noviembre. In: Spanish National Bulletin (BOE); 2010. (in Spanish).

[41] Cano, J. J. Introducción a la informática forense. Revista Asociación Colombiana de Ing de Sistemas (ACIS). 1996;96:64–73.

[42] Llaneza, P. and Lázaro, F. Evidencias electrónicas: de la información a la prueba electrónica. Seguridad en Informática y Comunicaciones (SIC). 2009;(83):92–97.

[43] Rahman, S. U. and Hengartner, U. Secure crash reporting in vehicular Ad hoc networks. In: International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007.p.443 –452.

[44] Lin, X. et al. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. Vehicular Technology, IEEE Transactions on. 2007 nov;56(6):3442 –3456.

[45] Delaney, A. et al. Controversies and Speed Cameras: Lessons Learnt Internationally. Journal of Public Health Policy. 2005;(26).

[46] Police Enforcement Policy and Programmes on European Roads (PEPPER) project. Deliverable 10: Implications of innovative technology for the key areas in traffic safety: speed, drink driving and restraint systems; 2008.

[47] Keithy, L. ANPR System Performance. Parking Trend International. 2008;Available online at: http://www.parkingandtraffic.co.uk/Measuring ANPR System Performance.pdf.

[48] Bossom, R. European ITS Framework Architecture, Functional Viewpoint, Version 3. Available online at: http://www.frame-online.net;.

[49] European ITS Framework Architecture. Browsing Tool version 4.1; 2011.

[50] Onn, Y. et al. Privacy in the Digital Environment. Haifa Center of Law and Technology; 2005.

[51] Ribagorda, A. Aspectos técnicos de seguridad en la Ley 11/2007 y su Reglamento de desarrollo parcial (in Spanish). Administración electrónica y ciudadanos (Director José Luis Piñar Mañas). p.718 – 742.

[52] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. In: Spanish National Bulletin (BOE); 2007. (in Spanish).

[53] International Standards Organization (ISO). 13888-1 Information technology - Security techniques - Non-repudiation. Part 1:General. ISO standards. 2009;.

[54] Hubaux, J. -P. and Čapkun, S. and Luo, J. The security and privacy of smart vehicles. IEEE Security and Privacy. 2004;2(3):49–55.

[55] Kremer, S. and Markowitch, O. and Zhou, J. An Intensive Survey of Fair Non-Repudiation Protocols. Computer Communications. 2002;25:1606–1621.

[56] González-Tablas, A. I. and Alcaide, A. and Suárez-Tangil, G. and de Fuentes, J. M. and Barroso-Pérez, I. Towards a privacy-respectful telematic verification system for vehicle and driver authorizations. In: Eighth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2011); 2011. .

[57] Strassberger, C. and Adler, C. Putting Together the Pieces - A Comprehensive View On Cooperative Local Danger Warning. In: Proceedings 13th ITS World Congress; 2006. .

[58] International Organization for Standardization. ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. ISO; 1989.

[59] Society of Automotive Engineers (SAE). SAE J2735. Dedicated Short Range Communications Message Set Dictionary; 2009.

[60] Anckaert, B. and De Sutter, B. and Chanet, D. and De Bosschere, K. Information Security and Cryptology ICISC 2004. vol.. 3506 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg.p.7–10.

[61] US Department of Transportation. IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE). Institute of Electrical and Electronics Engineers; 2009.

[62] Intelligent Transportation Systems Commitee. IEEE Standard Specifications for Public-Key Cryptography- Amendment 1: Additional Techniques. IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000). p.1–159.

[63] Mackay, David J. C. Information Theory, Inference and Learning Algorithms. Cambridge University Press; 2003.

[64] Robinson P. Middleware for Fair Non-repudiable Interactions. In: 6th Annual Postgraduate Symposium on the Convergance of Telecommunications, Networking and Broadcasting; 2005. .

[65] Fonseca, E. and Festag, A. and Baldessari, R. and Aguiar, R. L. Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In: Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE.p.3400 –3405.

[66] Ferrer-Gomilla, J. -L. and Onieva, J. A. and Payeras, M. and Lopez, J. Certified electronic mail: Properties revisited. Computers and Security. 2010;29(2):167 – 179.

[67] Raya, M. and Papadimitratos, P. and Aad, I. and Jungels, D. and Hubaux, J. P. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications. 2007;25(8):1557–1568.

[68] Toll Collect. Frequently Asked Questions, available at: http://www.toll-collect.de/faq/tcrdifr004-4_ kontrolle.jsp. Toll Collect; accessed in 2012.

[69] Papadimitratos, P. and Buttyan, L. and Holczer, T. and Schoch, E. and Freudiger, J. and Raya, M. and Zhendong Ma and Kargl, F. and Kung, A. and Hubaux, J. -P. Secure vehicular communication systems: design and architecture. Communications Magazine, IEEE. 2008 november;46(11):100 –109.

[70] Abumansoor, O. and Boukerche, A. A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET. Vehicular Technology, IEEE Transactions on. 2012 jan;61(1):275 –285.

[71] Li, F. and Wang, Y. Routing in vehicular ad hoc networks: A survey. Vehicular Technology Magazine, IEEE. 2007 june;2(2):12 –22.

[72] Mahmoud, M. E. and Shen, X. PIS: A Practical Incentive System for Multihop Wireless Networks. Vehicular Technology, IEEE Transactions on. 2010 oct;59(8):4012 –4025.

[73] Marti, S. and Giuli, T. J. and Lai, K. and Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking. MobiCom '00. New York, NY, USA: ACM.p.255–265.

[74] Bai, F. and Krishnan, H. Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications. In: Intelligent Transportation Systems Conference, 2006. ITSC '06. IEEE.p.355–362.

[75] Q-Free. CVIS platform– The future of Intelligent Transport Systems. CVIS project; 2010.

[76] Bunch, J. et al. Intelligent Transportation Systems Benefits, Costs, Deployment, and Lessons Learned Desk Reference: 2011 Update. US Department of Transportation; 2011.

[77] Festag, A. and Papadimitratos, P. and Tielert, T. Design and performance of secure geocast for vehicular communication. Vehicular Technology, IEEE Transactions on. 2010;59(5):2456–2471.

[78] Schoch, E. and Kargl, F. On the efficiency of secure beaconing in VANETs. In: Proceedings of the third ACM conference on Wireless network security. WiSec '10. New York, NY, USA: ACM.p.111–116.

[79] Johnson, N. and Jajodia, S. Steganalysis of Images Created Using Current Steganography Software. vol.. 1525 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg.p.273–289.

[80] Petitcolas, F. A. P. and Anderson, R. J. and Kuhn, M. G. Information hiding-a survey. Proceedings of the IEEE. 1999;87(7):1062–1078.

[81] Kenney, J. B. Dedicated Short-Range Communications (DSRC) Standards in the United States. Proceedings of the IEEE. 2011 july;99(7):1162 –1182.

[82] Fastenrath, U. Floating car data on a larger scale. DDG Gesellschaft fr Verkehrsdaten mbH; 2008.

[83] Viriyasitavat, W. and Tonguz, O. K. and Bai, F. Network Connectivity of VANETs in Urban Areas. In: IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. SECON '09.p.1 –9.

[84] M. Behrisch, M. and Bieker, L. and Erdmann, J. and Krajzewicz D. SUMO - Simulation of Urban MObility: An Overview. In: SIMUL 2011, The Third International Conference on Advances in System Simulation. Barcelona, Spain.p.63–68.

[85] Martinez, F. J. and Cano, J. -C. and Calafate, C. T. and Manzoni, P. CityMob: A Mobility Model Pattern Generator for VANETs. In: IEEE International Conference on Communications Workshops, ICC Workshops '08.p.370 –374.

[86] Deliverable 2: Integrated enforcement architecture. Fully Automated Integrated Road control (FAIR) project; 2006.

[87] Deliverable 17. Final Report. PEPPER project; 2008.

[88] University of Calgary. In-vehicle intelligent transportation system (ITS) countermeasures to improve older driver intersection performance. University of Calgary; 2006.

[89] Kovacs, A. et al. Use Cases and System Requirements (Deliverable 2.2). CVIS project; 2006.

[90] Raya, M. and Aziz, A. and Hubaux, J. -P. Efficient secure aggregation in VANETs. In: Proceedings of the 3rd international workshop on Vehicular ad hoc networks. VANET '06. New York, NY, USA: ACM.p.67–75.

[91] International Standards Organization (ISO). ISO 10711:2012. Intelligent Transport Systems – Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors; 2012.

[92] Spanish Government. Real Decreto 818/2009 por el que se aprueba el Reglamento General de Conductores. In: Spanish National Bulletin. 138; 2009. (in Spanish).

Appendix A

Acronyms and abbreviations

Acronym	Term
AA	Allegation Analyser
Adj	Adjudicator
ApA	Appeal Analyser
ARI	Appeal Result Issuer
CA	Certification Authority
CEA	CounterEvidence Analyser
CSA	Controle et Sanction Automatisée
DCP	Designated-as-offender Contact Point
DEV	Dirección Electrónica Vial
DPDM	Designated-as-offender Personal Data Manager
DR	Data Requester
DSRC	Dedicated Short Range Communications
EA	Evidence Analyser
EC	Evidence Collector
EM	Evidence Manager
ESTRADA	EStación de TRAtamiento de Denuncias Automatizadas
EUCARIS	EUropean CAR and driver Information System
EVIGEN	EVIdence GENeration protocol
FFI	Final Fine Issuer
HMI	Human-Machine Interface
HSM	Hardware Security Module
IFI	Initial Fine Issuer
IntFI	Intermediate Fine Issuer
ITS	Intelligent Transport System

Acronym	**Term**
LDA	Liable Driver Analyser
MI	Message Issuer
N	Notifier
NAdS	Notification Advertisement System
NMan	Notification Manager
NP	Notification Provider
NR	Notification Receiver
NRS	Notification Receiving System
NS	Notification Sender
OBU	On-Board Unit
PA	Process Analyser
PDM	Process Data Manager
RSU	Road-Side Unit
SAE	Secure Application Environment
TPM	Trusted Platform Module
VANET	Vehicular Ad-hoc Network
VDM	Vehicle Data Manager
VERA2	Video Enforcement for Road Authorities 2 project
V2I	Vehicle to infrastructure communication
V2V	Vehicle to vehicle communication

Appendix B

Publications

This Section lists the references of published works that have been derived during the realization of this doctoral thesis. The preliminary work over which this thesis has been based are also introduced here.

1. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. "Hacia un sistema preventivo del exceso de velocidad", X Reunión Española sobre Criptografía y Seguridad de la Información (RECSI), 2008. ISBN: 978-0-7695-2932-5

2. de Fuentes, J.M.; González-Tablas, A.I.; Ramos, B.; Ribagorda, A. "Protocolo de creación de evidencias en entornos vehiculares", V Congreso Iberoamericano de Seguridad Informática (CIBSI), 2009.

3. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. "Witness-based evidence generation in Vehicular Ad-Hoc Networks", 7th Embedded Security in Cars Conference (ESCAR), 2009.

4. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. "Autenticación y privacidad en redes vehiculares", Novática (202), March 2010.

5. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. "Authentication and privacy in vehicular networks", UPGRADE (IX), 6, March 2010.

6. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. "Modelo de procedimiento sancionador electrónico aplicado al control del tráfico vehicular", XI Reunión Española sobre Criptografía y Seguridad de la Información (RECSI), 2010. ISBN: 978-84-693-3304-4

7. de Fuentes, J.M.; González-Tablas, A.I.; Ribagorda, A. “Overview of security issues in Vehicular Ad-hoc Networks”, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, 2011.

8. de Fuentes, J.M.; González-Tablas, A.I.; López Hernández-Ardieta, J.; Ribagorda, A. “Towards an automatic enforcement for speeding: enhanced model and ITS realization”, IET Intelligent Transport System, to appear (accepted May 2012).

9. de Fuentes, J.M.; Blasco, J.; González-Tablas, A.I.; Hernández-Castro, J.C. “Applying steganography in Vehicular Ad-Hoc Networks to enable covert reporting of misbehaving vehicles”, IET Intelligent Transport System, under review (1st round). Status date: January 2012.

10. de Fuentes, J.M.; González-Tablas, A.I.; González-Manzano, L.; Ribagorda, A. “Diseño de un protocolo para el envío de notificaciones de denuncias por hechos de circulación al vehículo a través de tecnologías ITS”, XII Congreso Español de Sistemas Inteligentes de Transporte, 2012

Appendix C

Specification of the data exchanges produced in the proposed model

```
begin
    Any witness stakeholder → Evidence collector (EC) : initial evidence (Traffic environment detection)
    EC → Process data manager (PDM), Evidence Analyser (EA) : initial evidence (Initial evidence transfer)
    if the offence is not reported by a police officer then
        EA → Vehicle Data Manager (VDM): Vehicle identifier (e.g. number plate, EVI) (Vehicle and owner / usual driver data request)
        VDM → EA: Vehicle data, owner or usual driver identifier (Owner or usual driver data response)
        EA → Designated-as-offender personal data manager (DPDM) : Owner or usual driver identifier (Personal data completion request)
        DPDM → EA: Owner or usual driver personal data: name, address, type of driving licence. Offending record(s): infringed rule(s), demerit points credit. (Personal data completion response)
        EA → Initial Fine Issuer (IFI) : initial evidence, Vehicle data, Offending record(s), Owner/usual driver personal data, evidence analysis result (Initial evidence verification result)
    else
        EA → DPDM: Offender identifier (Personal data completion request)
        DPDM → EA: Offending record(s): infringed rule(s), demerit points credit. (Personal data completion response)
        EA → Initial Fine Issuer (IFI) : initial evidence, Offending record(s), evidence analysis result (Initial evidence verification result)
    IFI → Notifier → PDM, Offence-related stakeholder : Initial fine (Fine notification)
```

Algorithm 12: Process starting

```
begin
    # Allegation identifying another person as the offending driver
    if the vehicle owner or usual driver was identified as the designated-as-offender
    and she is not the offending driver then
        Vehicle owner/usual driver → Designated-as-offender contact point
        (DCP) → Liable Driver Analyser (LDA): Allegation identifying the
        offending driver (Offender identification request)
        # The following action only happens if the LDA determines that it is a
        plausible identification. Otherwise, the criminal law may be applied
        LDA → Initial Fine Issuer : Offending driver personal data (Offender
        identification transfer)
        GO TO else case in Starting algorithm
    # Counterevidence creation and transfer. This part should be repeated if
    multiple counterevidences are involved
    Any offence-related stakeholder → Data Requester (DR) → Selected
    witness stakeholder:
    Offender data: Designated-as-offender id. or vehicle number plate,
    Offence characterization: date, time, place.
    Requested counterevid. description: type (testimony, graphical proof, probatory
    element), witness stakeholder identifier (Data request)
    Selected witness stakeholder → DR → Offence-related stakeholder :
    Requested counterevidence data, witness stakeholder identifier, time of evidence
    (Counterevidence data retrieval)
    Offence-related stakeholder → Designated-as-offender Contact Point
    (DCP) → Process Data Manager (PDM), CounterEvidence Analyser
    (CEA) : Counterevidence (Counterevidence transfer)
    # Allegations are autonomously created by the offence-related stakeholder. They
    are also transferred for evaluation
    Offence-related stakeholder → DCP → PDM, Allegation Analyser
    (AA) : Allegation (Allegation transfer)
    # Counterevidence/allegation analysis. First part: additional data retrieval (if
    needed)
    CEA / AA → DR → Selected witness stakeholder: Additional data
    request: Offence subject (one of: offence context, offender behaviour or road
    traffic status), offence context (place, date, time, offender vehicle identification),
    witness stakeholder identifier. (Additional test for contrasting the counterevid.
    and alleg. (request))
    Affected witness stakeholder → DR → PDM, CEA / AA: Additional
    data response: Witness stakeholder identifier, requested data, time of response.
    (Additional test for contrasting the counterevid. and alleg. (result))
    # Counterevidence/allegation analysis. Second part: assessment. Intermediate
    fine issuance
    CEA / AA → Intermediate Fine Issuer (IntFI) : Counterevidence(s),
    allegation(s), additional requested data, evaluation result of these elements and
    their legal relevance (Assessment transfer)
    # This only happens if additional data retrieval was needed
    IntFI → Notifier → PDM, Offence-related stakeholder: Intermediate fine
    (Intermediate fine notification)
```

Algorithm 13: Preliminary investigation

```
begin
    if the Intermediate fine was notified to the offender (see Algorithm 13) then
        Offence-related stakeholder → Designated-as-offender Contact Point (DCP) → Process Data Manager (PDM), Process Analyser (PA) : Allegation (Allegation transfer)
    PA → PDM : Legal process identifier (Process data retrieval (request))
    PDM → PA : Initial fine, intermediate fine, allegation(s), counterevidence(s), Additional data retrieved in the preliminary investigation. (Process data retrieval (response))
    PA → Final Fine Issuer (FFI): Process revision, including the recent allegations (if any) and assessment of their relevance in the process (Allegation evaluation)
    FFI → PDM, Notifier → Offence-related stakeholder: Final fine (Final resolution notification)
    if the offence is considered as serious then
        # According to the Spanish legislation, it must be annotated in the Designated-as-offender personal data manager in case that is considered a serious (i.e. not minor) offence [92].
        FFI → Designated-as-offender personal data manager (DPM) : Offender identifier, legal process identifier, infringed rule, demerit points credit (Offence record annotation)
```

Algorithm 14: Process resolution

```
begin
    Offence-related stakeholder → Designated-as-offender Contact Point (DCP) → Process Data Manager (PDM), Appeal Analyser (ApA): Appeal (Appeal transfer)
    ApA → PDM : Legal process identifier (Process data retrieval request)
    PDM → ApA : Initial fine, intermediate fine, final fine, allegation(s), counterevidence(s), Additional data retrieved in the preliminary investigation. (Process data retrieval response)
    ApA → Appeal Result Issuer (ARI) : Appeal, Appeal assessment: reasoned appeal relevance evaluation. (Appeal evaluation transfer)
    ARI → Notifier, PDM → Offence-related stakeholder : Appeal result (Appeal resolution notification)
```

Algorithm 15: Process appealling

Appendix D

Resumen extendido