A Trust-driven Privacy Architecture for Vehicular Ad-Hoc Networks

Jetzabel M. Serna-Olvera

Computer Architecture Department

Universitat Politècnica de Catalunya

A thesis submitted for the degree of

Doctor of Philosophy in Computer Architecture

2012

Advisor: Prof. Manel Medina

Co-advisor: PhD. Jesús Luna

Internal examiner: Prof. Leandro Navarro

blank

I would like to dedicate this thesis to my loving son and husband, for being an important part of my life, and whose patience, confidence and love, gave me the strength and courage to never give up.

Acknowledgements

I must first thank my supervisor Prof. Dr Manel Medina for discussing and supervising my thesis work, and for giving me the opportunity to be part of the Network Security Group.

Thanks to Dr. Jesús Luna for supervising my work and for his useful feedback, and support during these years.

I am grateful to Trinidad Carneros, and Prof. Dr. Leandro Navarro for helping me in every matter towards the adaptation of living and studying in Spain.

A recognition to the institutions that supported this work: The Agència de Gestió d'Ajuts Universitaris i de Recerca (AGAUR), the Universitat Politècnica de Catalunya (UPC), my particular thanks for granting me the opportunity to study the PhD degree in Barcelona.

My especial thanks the Università degli Studi di Napoli Federico II, and in particular, to Valentina Casola and Massimiliano Rak, for their important collaboration and support during the research internship in Italy.

I would like to express my gratitude to my family Maricela Olvera, J. Jesús Olvera, Rosa María Olvera, Roberto Morales, Jorge Morales and Anna Maschkowkaja, for their love and patience, and for providing me all the technical resources and support to begin and finalize my doctoral studies in Spain.

Finally, I am also grateful to my friends Jorge Crespo, Alejandro Uriza, Thania Rendón, Paul Bourne, Aída Zavala, Dr. Chuchito, Patricia Rodríguez and Víctor Rodríguez for their friendship and their collaboration with ideas and stimulating discussions, for their help and support all this time.

Abstract

Vehicular Ad-Hoc NETworks (VANETs) are an emerging technology which aims to improve road safety by preventing and reducing traffic accidents. While VANETs offer a great variety of promising applications, such as, safety-related and infotainment applications, they remain a number of security and privacy related research challenges that must be addressed.

A common approach to security issues widely adopted in VANETs, is the use of Public Key Infrastructures (PKI) and digital certificates in order to enable authentication, authorization and confidentiality. These approaches usually rely on a large set of regional Certification Authorities (CAs). Despite the advantages of PKI-based approaches, there are two main problems that arise, *i)* the secure interoperability among the different and usually unknown- issuing CAs, and *ii)* the sole use of PKI in a VANET environment cannot prevent privacy related attacks, such as, linking a vehicle with an identifier, tracking vehicles "big brother scenario" and user profiling. Additionally, since vehicles in VANETs will be able to store great amounts of information including private information, unauthorized access to such information should be carefully considered.

This thesis addresses authentication and interoperability issues in vehicular communications, considering an inter-regional scenario where mutual authentication between nodes is needed. To provide interoperability between vehicles and services among different domains, an Inter-domain Authentication System (AS) is proposed. The AS supplies vehicles with a trusted set of authentication credentials by implementing a near real-time certificate status service. The proposed

AS also implements a mechanism to quantitatively evaluate the trust level of a CA, in order to decide on-the-fly if an interoperability relationship can be created.

This research work also contributes with a Privacy Enhancing Model (PEM) to deal with important privacy issues in VANETs. The PEM consists of two PKI-based privacy protocols: *i)* the Attribute-Based Privacy (ABP) protocol, and *ii)* the Anonymous Information Retrieval (AIR) protocol. The ABP introduces Attribute-Based Credentials (ABC) to provide conditional anonymity and minimal information disclosure, which overcome with the privacy issues related to linkability (linking a vehicle with an identifier) and vehicle tracking (big brother scenario). The AIR protocol addresses user profiling when querying Service Providers (SPs), by relying in a user collaboration privacy protocol based on query forgery and permutation; and assuming that neither participant nodes nor SPs could be completely trusted.

Finally, the Trust Validation Model (TVM) is proposed. The TVM supports decision making by evaluating entities trust based on context information, in order to provide *i)*access control to driver and vehicle's private information, and *ii)* public information trust validation.

Contents

List of Figures

Chapter 1

Introduction

Vehicular Ad-hoc NETworks (VANETs) currently provide a prominent field of research, that aims at improving everyday road safety and comfort. To achieve this, the development of several potential applications is envisioned. Such applications, will not only promise to provide extraordinary benefits, but will also represent important security challenges, especially due to the unique characteristics of VANETs. In this chapter, the basics of VANETs will be briefly introduced, followed by a discussion about the main reasons why, despite their potential benefits, VANETs also raise important security and privacy concerns that must be properly addressed. The problem statement and the main contributions of this thesis are presented in subsequent sections, and finally, at the end of this chapter, the thesis organization is outlined.

1.1 Motivation

Road traffic injuries are currently the ninth leading cause of death in the world, killing nearly 1.3 million people annually. Unless effective action is taken, road accidents are predicted to become the fifth leading cause of death by 2030 (WHO, 2012). Intelligent Transportation Systems (ITS)(Committee, 2007) aim to provide innovative services that will potentially benefit traffic management. As the technical basis of ITS, VANETs offer the possibility of significant improvements in order to mitigate vehicular accidents and enable a wide range of safety and mobility applications promising extraordinary benefits.

VANETs consist of mobile and fixed nodes represented by vehicles and Road Side Units (RSUs) (Figure 1.1) communicating among each other and enabling the exchange of different kinds of information (Zarki *et al.*, 2002). Thus, as previously mentioned, their successful deployment will allow the implementation of several applications intended to drastically reduce the number of road fatalities by improving overall road safety, as well as being capable of providing value added services to enhance driver comfort.

In safety-related applications, exchanged information plays a vital role, in particular, in traffic safety. Many of these applications may demand the driver's awareness and even his/her reaction. If a driver is supposed to react instantly, e.g., in the case of road accidents or life-critical warning messages, since lives could depend on these applications, the information must be accurate and truthful, and vehicles should be able to *(i)* ensure that the information received is correct, *(ii)* verify that the sender has been authenticated and authorized, and therefore can be trusted. To assure both aspects, security measures are essential and must be taken into consideration. While increasing road safety is its main goal, VANETs also offer other applications such as location-based services while en route, which adversaries could exploit by injecting wrong information into the network or by gaining information from value added services and consequently threaten drivers' privacy and safety. Moreover, since vehicles in a VANET will be provided with storage and processing capabilities, avoiding unauthorized information disclosure should also be carefully addressed. The lack of security could consequently jeopardize the potential benefits expected from VANET applications, thus, a set of security goals should be satisfied in order to prevent attackers from inserting or modifying exchanged (e.g., life-critical) information, without compromising drivers' privacy but able to establish their liability in case of accidents.

In summary, vehicular communications should not become a weak link in terms of security and privacy, but should provide users with, at least, the same level of protection that is currently afforded without vehicular networks. In the following section, current research issues identified around this topic will be discussed.

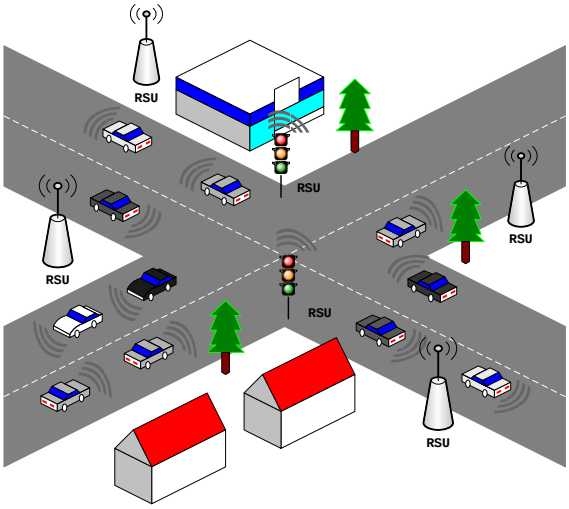

Figure 1.1: VANET system model

1.2 Problem Statement

The aim of VANETs is to provide safety and comfort, thus, in vehicular communications, the information exchanged among vehicles plays a fundamental role. Identifying the context in which information could be trusted is a relevant aspect to be considered. In particular, for safety-related applications, the information transmitted among vehicles is considered critical, thus, timely and accurate exchange of this information could prevent a great number of fatal road accidents. However,if an attacker manipulates the information could potentially cause harm; therefore, in order to prevent potential attacks, implementing security measures is of the utmost importance. To overcome this, the adoption of Public Key Infrastructure (PKI) technology, which has been proven to be a suitable solution in other distributed environments, has been considered. The implementation of PKI will enable the establishment of secure communication channels, by providing services needed to prevent a wide range of security attacks. Current PKI systems consist of a Central Authority (CA) responsible for registering users and issuing credentials (containing the corresponding private and public key-pair).

In VANETs, it is envisioned that vehicles will be registered with their own regional CA, and therefore, a common architecture will require a wide range of CAs

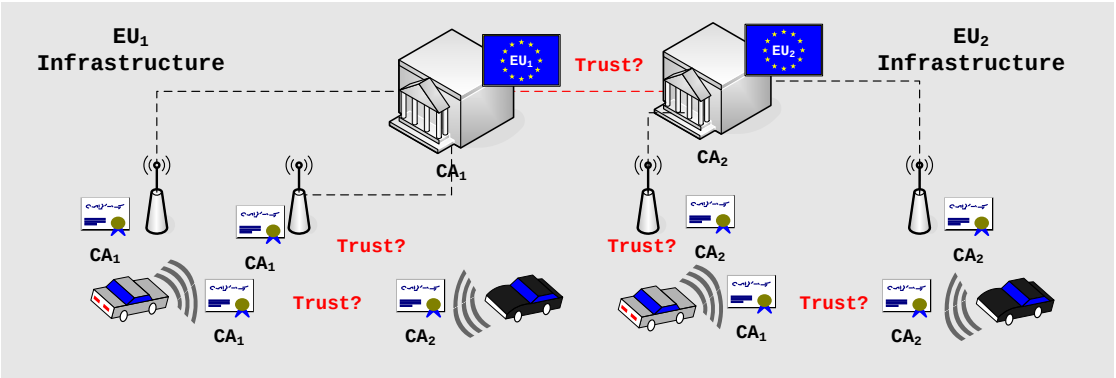

Figure 1.2: Interoperability among CAs, to provide inter-domain authentication when vehicles travel to different domains

within regional scopes (Figure 1.2). However, by following the implementation of several CAs, **how will authentication and authorization be performed when vehicles move between two different geographical regions?**. It is assumed that when a vehicle travels to a different geographical region or domain, a mutual authentication and trusted communication will be achieved thanks to previous cross-certification agreements (mostly manual). Nevertheless, since certificate revocation is also the responsibility of the issuing CA, a disadvantage of cross-certification is that, it is not possible to obtain up-to-date revocation information resulting in a vulnerability window for the relying party, which raises the question on **how to automatically perform "cross-certification"** and *i)* validate trust among unknown CAs and *ii)* validate in near-real time a VANET's node certificate status.

Apart from the revocation issues just mentioned, and despite the benefits of enabling the use of PKI technologies in VANETs, the sole use of PKI cannot ensure privacy, which also plays an important role in any VANET architectural solution. A few examples of privacy problems that should be faced in a typical VANET are: *(i)* linking a person and an identifier, *(ii)* tracking a specific node, and, since vehicles in a VANET will also benefit from accessing a wide number of added value applications offered by different Service Providers (SPs), *(iii)* the big brother scenario of gathering detailed statistics about movement patterns and services requested by vehicles could also be a threat. To address privacy issues,

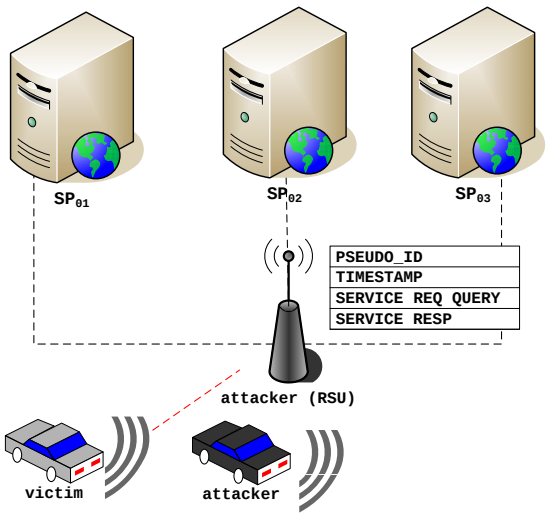

Figure 1.3: Big brother scenario, an attacker (vehicle or RSU) collecting information from a vehicle's requests to different service providers at different times $(t_1, t_2, ..., t_n)$

the general approach is the implementation of temporary certificates based on pseudonyms, which are an interesting, but yet only a complementary solution. Pseudonyms could prevent linking a person to an identifier, but cannot prevent an attacker from collecting another user's related data; the passive collection of communication information regarding vehicle activities (e.g. locations and contents of queries to services provided by the infrastructure), could lead to user profiling (Figure 1.3). Moreover, private information stored in vehicles should only be disclosed to authorized parties (Figure 1.4).

The general principle in VANET privacy is that information of the vehicle and the driver should be protected against private citizens and law enforcement agencies, only disclosing it to authorized parties, where privacy should be conditional to specific scenarios (liability). Given the above mentioned scenario, important questions to be solved are *i)* how to avoid user profiling when requesting services to the infrastructure? *ii)* how to provide conditional anonymity and unlinkability? and *iii)* how to prevent unauthorized information disclosure among vehicles?.

Finally, due to the high mobility of vehicles, the system introduces different

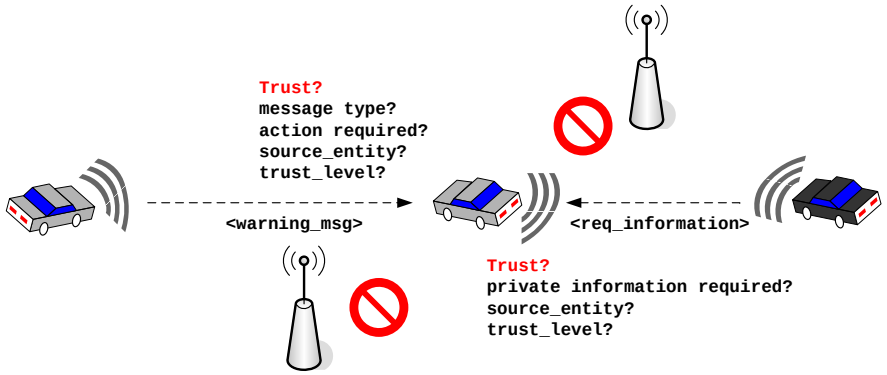

Figure 1.4: Information trust validation in vehicle to vehicle communication - no infrastructure available

network constraints that should be taken into account for the overall security design. A successful deployment must process and transmit the information within the timing and communications parameters limited by the network, thus, the need to carefully design a suitable security solution, able to meet the VANETs' performance requirements, especially those related to the bandwidth usage and the processing overhead. Thus, the main purpose of this research work is to deal with the aforementioned security and privacy issues, and prevent abuse by implementing a PKI-based solution that addresses the interoperability issues among different realms and ensure the privacy of the involved entities in VANETs. The specific contributions of this thesis are described in the following section.

1.3 Specific Contributions

The main contributions of this thesis consist in addressing important security and privacy challenges in Vehicular Ad hoc Networks by proposing a privacy-aware security framework (Figure 1.5). In particular, to overcome the security and privacy issues discussed in Section 1.2, we point out the main contributions:

- **Authentication System (AS)** is a geo-location based trust model, which provides PKI-interoperability (Figure 1.2), allowing vehicles to perform authentication among untrusted domains. The AS implements the certificate

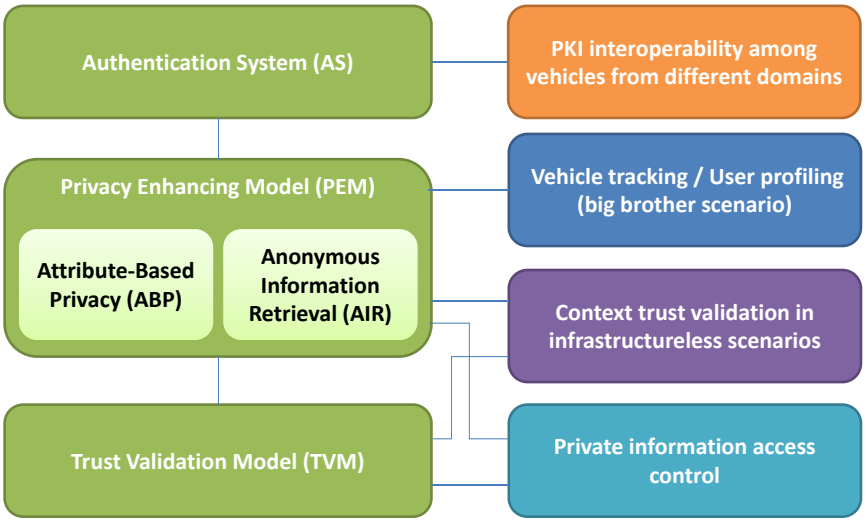

Figure 1.5: Privacy-aware Security Framework

validation process, and automatically builds a dynamic CA federation to provide cross-certification via policy mapping.

- **Attribute-Based Privacy (ABP)** protocol implements Attribute-Based Credentials (ABC) to provide minimal information disclosure by selectively disclosing attributes to any relaying party such as a service provider (SP) and prevents vehicle tracking (Figure 1.3), especially while requesting services from the infrastructure.

- **Anonymous Information Retrieval (AIR)** implements query permutation and query forgery to avoid user profiling. Taking advantage of user collaboration, the AIR protocol avoids query-user association, and overcomes potential privacy issues derived by eavesdropping (Figure 1.3). Moreover the protocol has been designed on the basis that neither the participating nodes nor the SP can be trusted.

- **Trust Validation Model (TVM)** is a model which consists of the implementation of context-based policies to *i)* prevent unauthorized access to vehicles private information and *ii)* validate the context of the received information and the trust level of the source nodes to be able to automatically

decide if the message could be trusted (Figure 1.4). Firstly, TVM classifies the type of information contained in the vehicle and the type of messages to be exchanged, by assigning different labels to the information according to its sensitivity level. Secondly, it validates the sender or requestor's trust level, according to a set of attributes previously assigned and mainly based on the role and the type of entity, which is achieved thanks to the proposed privacy enhancing model.

1.4 Thesis Organization

This thesis is organized as follows:

Chapter 2 Provides an overviews of the basic concepts of Vehicular Ad Hoc Networks. Current projects and efforts, along with the security and privacy issues that are inherent in VANET technologies, are also discussed in this chapter.

Chapter 3 Presents and analyzes the related state-of-the-art approaches, focusing on security and privacy in VANETs.

Chapter 4 Introduces an Inter-domain Authentication System to provide trust establishment and authentication among vehicles belonging to unknown domains.

Chapter 5 Proposes a Privacy Enhancing Model (PEM) that consists of an Attribute-Based Privacy (ABP) protocol which introduces Attribute-Based Credentials (ABC) to anonymously communicate and prevent vehicle tracking. In order to prevent user profiling, the PEM model introduces the Anonymous Information Retrieval (AIR) protocol that implements query forgery and permutation to provide minimal information disclosure when requesting services to the Service Providers (SPs).

Chapter 6 Defines a context-based Trust Validation Model (TVM), by implementing context-based policies to *i)* avoid unauthorized private information access and *ii)* allow information trust validation even when no infrastructure is available.

Chapter 7 Analyzes the trade-offs among security, privacy and performance related to the proposed model.

Chapter 8 Gives the main conclusions and future research directions in VANET security and privacy.

Chapter 2

Background

2.1 Vehicular Ad hoc Networks

Vehicular Ad hoc NETworks are a subgroup and one of the most relevant representations of Mobile Ad hoc NETworks (MANETs). Basically MANETs consist of autonomous collections of mobile nodes, represented by independent wireless devices acting as both end systems and routers that move independently forming unpredictable and highly dynamic topologies just as shown in Figure 2.1. In VANETs' communication vehicles are equipped with On-Board Units (OBUs) able to communicate to the infrastructure mainly represented by Road Side Units (RSUs) located along the roads.

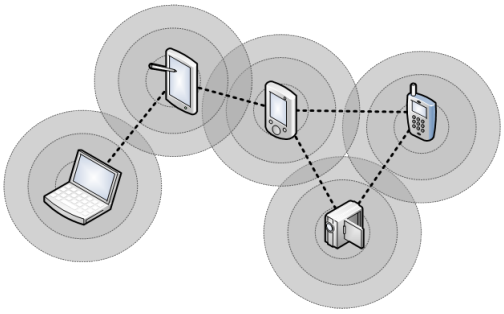

Figure 2.1: Mobile Ad Hoc Network

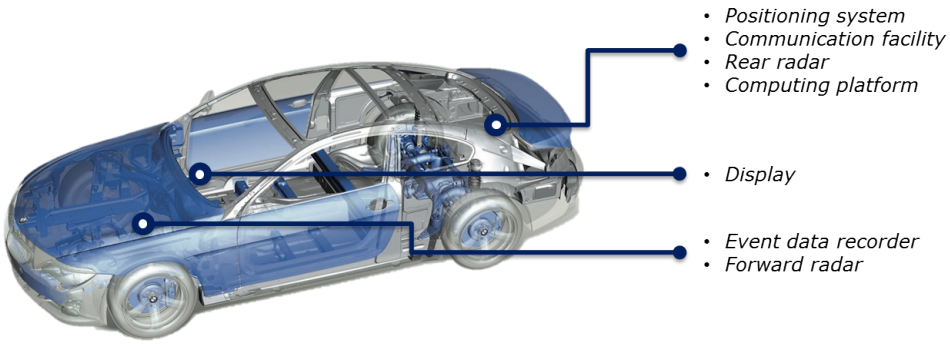

Figure 2.2: Smart-vehicle

2.1.1 Communication Model

It is envisioned that in the coming years 40% of all vehicular components will be electronic, with this integration, vehicles referred as "smart-vehicles" (Hubaux *et al.*, 2004), will be equipped with processing, recording and communication features, capable of processing and storing a great amount of information (Figure 2.2)

The communication among both kinds of VANETs nodes is commonly classified as vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) Figure 2.3, and according to the Dedicated Short Range Communications - DSRC standard (Armstrong, 2012a), VANETs are capable of communicating at data rates from 6-27Mbps at a maximum transmission range of 1000m, thus, enabling nodes to exchange all kinds of application-related information.

2.1.1.1 Projects and Organization

The networking community is at present putting significant effort into investigating inter-vehicle communications. The areas of current research range from the low layer protocols design to the implementation of a wide range of applications and mechanisms for the effective deployment of vehicular ad-hoc networks. The development of these vehicular communication systems is driven by a number of national and international activities such as, the Car-to-Car Communication consortium (C2C-CC) (C2CCC, 2012) and the California Partners of Advanced

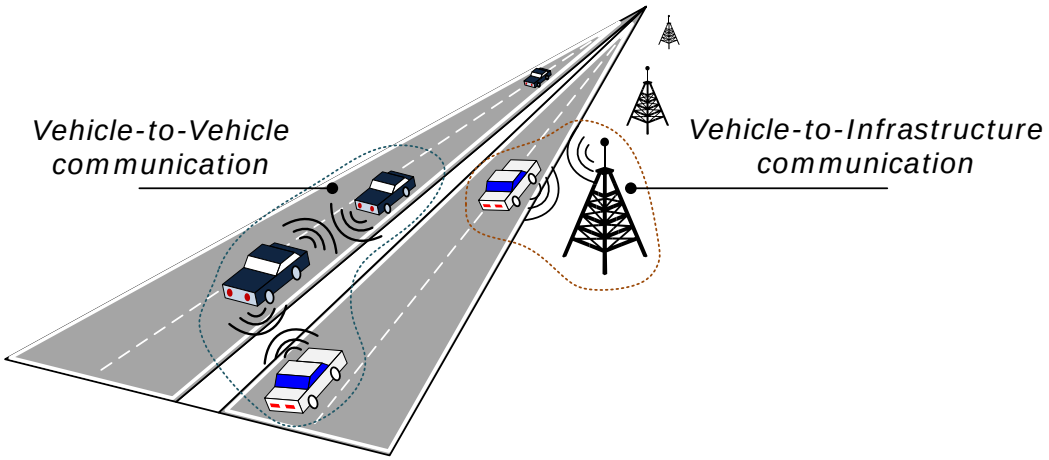

Figure 2.3: Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication

Transit and Highways (PATH, 2012). These organizations focus on building high performance architectures and extracting application specific functionality to be integrated into the VANET system (i.e. application specific packet routing).

2.1.1.2 Communication Standards

In vehicular communications, vehicle are able to share different communication channels which are highly unreliable and generally with a limited bandwidth. The need of new protocols and mechanisms to guarantee effective, reliable, and secure communications are needed. The IEEE 802.11 (IEEE LAN/MAN Standards Committee – IEEE802, 2012) standard family provides wireless connectivity between v2v and v2i, however these standards have not considered VANET's unique characteristics (Section 2.1.1.3 such as driving speeds, traffic patterns, and driving environments. To address these requirements, recently, the Dedicated Short Range Communication (DSRC) and the Wireless Access in Vehicular Environments (WAVE) which are the based on 802.11p and IEEE 1609 standards have been developed. The DSRC is based on the physical and MAC layer of the 802.11 standard, providing high data transfers and low communication latency in small communication zones. Taking advantage of the efforts done so far by the

ASTM2313 working group on DSRC they migrated to the IEEE 802.11 standard group and renamed the DSRC to IEEE 802.11p WAVE (Zeadally *et al.*, 2010). The WAVE standards define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure wireless communications required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed v2v and v2i communications in the licensed ITS band of 5.9 GHz (5.855.925 GHz). Additionally, IEEE 1609 is a higher layer standard on which IEEE 802.11p is based which allows homogeneous communications interfaces between different automotive manufacturers.

2.1.1.3 VANETs Features

As a subgroup of MANETs, VANETs share similar characteristics with other ad-hoc networks (Zarki *et al.*, 2002), but also possess' unique features that on one hand can influence positively on the deployment of several applications, and on the other hand represent an interesting challenge that must be carefully considered when designing any architectural solution. In the following, these particularities will be briefly described.

- Dynamic topology: Compared to conventional MANETs, nodes in VANETs could be easily distinguished by their variable and high speeds, together with the different trajectories that nodes are able to follow; communication links among them can only be established in a temporary fashion, resulting in continuous topology changes, i.e. the longer that vehicles are within the communication range (e.g. vehicles following similar trajectories), the longer that a particular topology is maintained.

- Mobility models: Despite the high mobility that is inherent to a VANET system, nodes mobility is bounded in speed and space, due to the fact that vehicles travel along pre-established trajectories (roads). The speed of vehicles is usually constrained by *i)* traffic lights, *ii)* routes intersections, *iii)* the speed of other vehicles, and by *iv)* general speed limits to control different kinds of urban areas. Moreover, since vehicles move along routes their movements could be predicted.

- Geolocalization capabilities: it is expected that most vehicles will have integrated, positioning devices such as Global Positioning System (GPS) receivers, along with other communication capabilities, enabling a potential range of location based applications.

- Low latency requirements: due to the dynamicity of the environment, and the delay constraints introduced by safety applications, the information exchanged among vehicles in VANETs is extremely time-sensitive, (e.g. alert messages to prevent about road conditions)

- Energy supply: an important difference between VANETs and other ad-hoc networks is that, in traditional MANETs, mobile nodes have limited power supply and processing resources, resulting in a major issue when designing services and applications that can be supported by each node, however, in VANETs resource constraints could be neglected, since in VANETs a running vehicle is able to provide sufficient battery power, more computational power resources are assumed. This feature is quite an important advantage for certain computational intensive tasks related with security (i.e. cryptography).

- Communication scenarios: communication in VANETs might be strongly dependent on the scenario (Guerrero-Ibez *et al.*, 2012), current research identifies two main scenarios *i)* highways, where vehicles travel at different speeds and unidirectional movement patterns can be observed, and *ii)* urban scenarios, where environmental elements play a fundamental role making v2v communications more complex.

The most challenging features inherent to a VANET system include the dynamic topology and the mobility models (vehicles moving at a variable and high speed and in different trajectories). On the other hand, thanks to the vehicle's geo-localization functionality and its "infinite" energy supply, VANETs are an enabler for a set of potential applications (further discussed in Section 2.1.1.4), but also rise important security and privacy issues that must be addressed.

2.1.1.4 Applications

In VANETs v2v and v2i communication, communicating nodes are either vehicles or RSUs, where the majority of nodes will consist in vehicles equipped with on-board units (OBUs) and fixed communication units along the road that can exchange information about traffic issues, road conditions and added value information, allowing the deployment of a wide range of applications that could be classified according to different aspects such as target, scenarios, or security objectives. In this thesis the most common classification initially employed by authors of (Raya & Hubaux, 2005),(Plossl *et al.*, 2006) has been adopted:

- Warning: Applications aimed to detect risky situations, such as the propagation of alerts in case of accidents. Vehicles exchange messages to inform each other about special events and dangers on the road, an example could be alarm signals from emergency vehicles in action, which is done by sending information such as current position, time and destination or desired route, where other vehicles could and must clear the way for the emergency vehicle.

- Traffic Management: a safety-related application where messages are primarily exchanged to inform about traffic congestion and road conditions in a given region with the main purpose of optimizing traffic. This expects safety in an indirect form basically by preventing potential accidents due to congestion.

- Added value applications: aimed at providing a wide range of services such as payment services, location-based services (e.g. finding the closest hotel, restaurant, etc.), and infotainment (e.g., Internet access, to offer e-mail, web browsing, video streaming, etc.).

As it can be inferred by the aforementioned applications, VANETs will be capable of offering a wide range of valuable services. However, along with the rise of VANETs, a set of security issues has also appeared, the importance of security and privacy implications will be further discussed in Section 2.1.2.

2.1.2 Security and Privacy

Vehicular systems are an important problem of our society, where the common goal is to reduce road accidents. Emerging technologies such as DSRC assigned for vehicle communications are promising to drastically reduce the number of traffic victims by providing early emergency warnings in various road situations (broadcasting routine messages over a single hop every 300ms with traffic related events information (NHTS, 2006)), as long as the exchanged messages are trustworthy they can greatly improve the overall road safety. A compromised VANET may disrupt the whole technology's applicability and acceptance, by, for example, causing life-threatening situations (i.e. false warnings that could results on road accidents), thus, any VANET solution must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission.

Privacy in VANETs is also a major concern, since vehicles are highly personal devices and they are kept for a long duration, and are expected to be able to store a lot of information including personal data; drivers should then be able to keep and control their personal and vehicle related information. Innocent looking data from several sources can be collected over long periods and be automatically evaluated to compromise privacy and produce several attacks (Dötzer, 2005). Once privacy is lost it is very difficult to re-establish that state of personal rights and the trust that people delivered into this technology (Kargl *et al.*, 2006). Thus, on one hand strong security mechanisms are needed to protect applications and users from possible attacks and on the other hand the protection of user's private information (not limited to identity) should be guaranteed.

2.1.2.1 Attacker Model

The classification of attackers can be done according to different characteristics such as location, motivation, etc., identifying a type of attacker facilitates considerably the study of his capacity, possible attacks and, consequently the harm that could be caused. Authors of (Raya & Hubaux, 2007), presented a general classification:

- Insider: is an authenticated member of the network

- Outsider: is considered by the other members of the network as an intruder.
- Malicious: this attacker seeks no personal benefits from the attacks and aims to harm.
- Rational: a rational attacker seeks personal profit and hence is more predictable.
- Active: an active attacker can generate packets or signals.
- Passive: A passive attacker contents himself with eavesdropping on the wireless channel.

Similar to other conventional MANETs, VANETs can also be vulnerable to a set of security attacks, which have been in different degree analyzed by authors of (Aijaz *et al.*, 2006), (Parno & Perrig, 2005) and (Raya & Hubaux, 2005). In the following, a classification of general attacks on VANETs corresponding to different security requirements needed in VANETs (de Fuentes *et al.*, 2010) is described:

Identification and Authentication An active, rational and insider attacker pretending to be one or multiple different entities could achieve an impersonation attack by *i)* claiming to be an authorized entity such as an emergency vehicle and propagate wrong information in the network, e.g. sending false information to alter traffic flow, slowing it down or getting a vehicle-free road, *ii)* in the same way a vehicle could pretend to be multiple entities reporting a false bottleneck to achieve the same purpose, *iii)* simple use of fictitious identities, to evade being responsible and legally obliged in case of an accident.

Privacy Linking a person with an identifier (ID disclosure) by a global passive observer overhearing the communication from vehicles (e.g an attacker RSU or vehicle on a parking lot), and afterwards could be able to distinguish *i)* a vehicle-identifier, which identifier belongs to which vehicle and as a result to which driver, *ii)* be able to monitor trajectories. With this information an attacker could then blackmail a driver if collected information contains compromising information.

Confidentiality an attacker represented by a vehicle or by a false RSU could get illegal access to confidential information, or a passive attacker eavesdropping the communication and gathering information on services requested by a vehicle.

Non-repudiation achieved mainly by rational attackers colluding to share the same credentials.

Availability Denial of service attacks are commonly done by active malicious attackers willing to bring down the network, these attacks include channel jamming and aggressive injection of dummy messages.

Data trust Inaccurate data calculation and sending affecting message reliability, performed by manipulating sent information mainly done by rational active attackers.

2.1.2.2 Security and Privacy Requirements

The successful deployment and public acceptance of VANET technology requires a security system able to prevent any generic attack. On vehicular networks, the system should use a secure and trusted communication infrastructure able to satisfy the following set of requirements (Kargl *et al.*, 2006) (Raya & Hubaux, 2007):

- Authentication: The authentication of the senders messages is needed to keep outsiders from injecting messages as well as misbehaving insiders.
- Integrity: All messages should be protected to prevent attackers from altering them, or in the worst-case scenario, to detect its modification.
- Confidentiality: There are application that require that only the sender and the intended receiver can access the content of a message.
- Access control: Vehicles and applications need fine-grained access rights. Sensitive information stored in vehicles should only be available for authorized parties.

- Availability: Transmitted messages must reach all necessary recipients despite the VANET's status.
- Non repudiation: A sender should not be able to deny the transmission of a message, specially in case of node's misbehavior, therefore to be able to prosecute misuse, non-repudiation is necessary.
- Privacy: The privacy of users should be enforced, it should not be possible to automatically obtain private information about drivers or vehicle's behavior and activities, linking the activities (services requested and location) to and identifier and an identifier to a person.

2.2 VANET's Public Key Infrastructure (VPKI)

Cryptography primitives are based on the use of keys employed to encrypt and decrypt information. There are two types of cryptography: *i)* symmetric-key cryptography, and *ii)* asymmetric-key cryptography also known as Public Key (PK). Symmetric-key cryptography has been discarded due to its scalability limitations, specially in complex systems such as VANETs where the increased number of vehicles introduces a significant key maintenance overhead. Opposite to Symmetric-key, in VANETs, Public Key cryptography has been adopted by many initiatives and in particular by the WAVE security standards (Section 2.1.1.2).

2.2.1 Basic Concepts

The basic PK provides an encryption and a signature scheme, both consisting of a private (Sk) and a public key (Pk).

In the encryption scheme an entity (A) publishes its (Pk); which will be used by others entities to encrypt a message (M) sent to entity (A), $C \longleftarrow e(M, Pk_A)$.

Upon reception of an encrypted message, entity (A) uses its (Sk) to decrypt and recover the original message (M), $d(C, Sk_A)$.

Opposite to encryption, the signature scheme, entity (A) signs a message (M) with its (Sk), $C \longleftarrow e(M, Sk_A)$ that will be verified only with by entities possessing entity's (Pk), $d(C, Pk_A)$.

Public Key Infrastructure or PKI is the general term for a security infrastructure which derives its name from Public Key Cryptography. PKI defines message formats and protocols that allow entitled to securely communicate claims and statements. The most commonly used assertions, are those that bind identity, attributes, and authorization statements either to keys or to identities.
The most popular PKI is defined by the IETF's PKIX working group (Housley *et al.*, 2002), which defines a security system used for identifying entities (users and resources) through the use of X.509 identity certificates. In this PKI, highly trusted entities known as Certificate Authorities (CAs) issue X.509 certificates where essentially a unique identity name and the public key of an entity are bound through the digital signature of that CA. As a trusted third party, the CA can be used as an introducer: through the proof of private key possession and the validation of the CA's issues X.509 certificates, entities are able to associate a trusted, unique identity name with the communicates claims and statements of others. General security requirements such as identification, authentication, non-repudiation and confidentiality, could be achieved with the implementation of a PKI-based solution.

2.2.2 Assumptions

Multiple CAs within regional scopes will be involved, and such CAs (national or regional) are mostly cross-certified (see Figure 2.4). Vehicles from different regional scopes should be able to verify each other. A CA will issue certified public/private key pairs to participating vehicles. To authenticate each other, vehicles sending a message will add digital signature at each of the messages, the digital signature will be generated by encrypted hash value of message using the private key. Vehicles receiving messages will verify the key used to sign the message, and the message's Certificate Authorities (CAs) Revocation is assumed to be done with the distribution of CRLs (Certificate Revocation Lists) that contain the most recently revoked certificates; CRLs will be updated and provided when infrastructure is available.

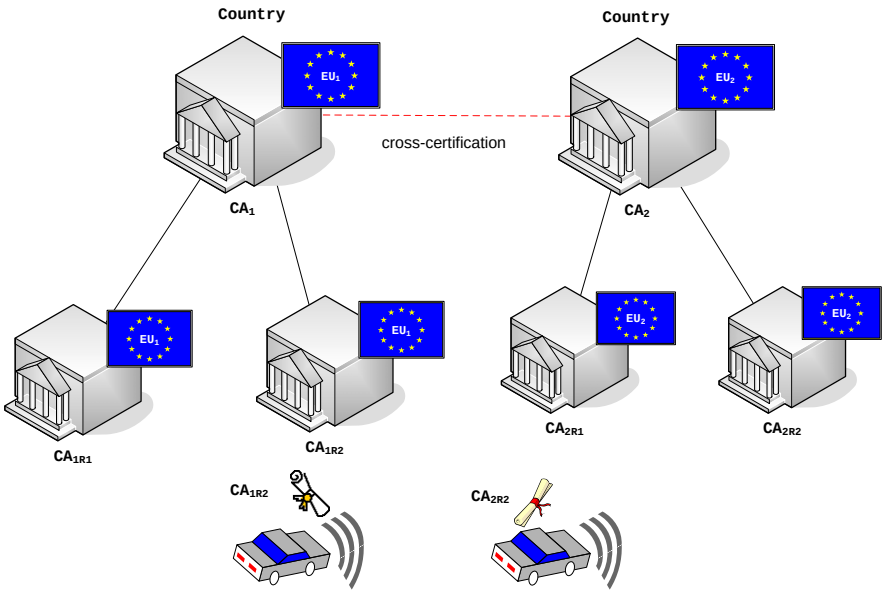

Figure 2.4: VPKI - Multiple CAs within regional scopes

2.2.3 Open Issues

An efficient VANET architecture is fundamental for being able to manage the whole certificate's life cycle (issue, distribution, validation and revocation). Yet, PKI-based solutions have overlooked the interoperability problems that could be derived from a multi-CA framework, by assuming explicit cross certification agreements. Revocation also represents an important scalability issue, CRLs can be very long due to the increased number of vehicles and their high mobility.

Moreover, as it has been previously discussed, the sole use of PKI, cannot prevent the privacy issues identified in (Section 2.1.2)

Chapter 3

State of the Art

Until recently, security in VANETs had been overlooked, yet, has drawn the attention of a wider research community. In this chapter, the main VANET security approaches found in the literature will be presented and further discussed.

3.1 Introduction

Since, in VANETs, access is granted by default, to be able to prevent any generic attack, the system should rely on a secure and trusted communication infrastructure able to satisfy a set of security requirements that include *i)* authentication, *ii)* integrity, *iii)* confidentiality, *iv)* availability, *v)* non-repudiation and *vi)* privacy. Thus, the important challenge is just finding the proper techniques and architectural solutions to be able to enforce privacy and security. In particular, authentication should be provided, even in the presence of nodes (vehicles) belonging to different "authentication realms" (usually linked with more than one geographical area), but without disregarding the privacy requirements inherent to VANETs users and applications.

An extensive study of security issues in vehicular networks has been presented by (Hubaux *et al.*, 2004),(Raya & Hubaux, 2005), (Papadimitratos *et al.*, 2006a) and among others (Wex *et al.*, 2008). Also authors of (Parno & Perrig, 2005) and (Aijaz *et al.*, 2006) provided a detailed analysis of general system security attacks on Inter-Vehicle Communication (IVC) and describe the main challenges

in securing vehicular networks, pointing out important system requirements concerning among others, privacy. In particular, a discussion of specific issues related to identity and privacy enhancing technologies for VC can be found in (Dötzer, 2005) and (Papadimitratos *et al.*, 2006b). According to current state of the art research, to implement a secure service access in vehicular networks the Wireless Access in Vehicular Environments (WAVE) standard (Committee, 2007) assumes that vehicles will be capable of running cryptographic protocols. Thus, the use of Public Key Infrastructures (PKI) and digital certificates have been proposed in (Papadimitratos *et al.*, 2007) as suitable solutions to overcome the authentication and authorization challenges in VANETs. However the implementation of PKI also rises interesting challenges.

3.2 Pseudonymity

The importance of privacy preservation for the public acceptance of VANET's technology has been highlighted by authors of (Dötzer, 2005) and (Gerlach, 2006), which have presented an extensive study on the implications of missing privacy. In particular, it has been remarked that, since, in general, digital certificates include information regarding the node's identity, the sole use of PKI cannot provide privacy. Thus, different approaches based on the use of pseudonyms [1] have been proposed. In VANETs pseudonymity refers to the use of digital pseudonyms as IDs and assuming that each pseudonym refers to exactly one holder. However, it is worth to mention that, the use of long-term credentials, even if combined with a pseudonym approach, opens up the possibility of linking a pseudonym with the vehicle's real identifier (e.g. an attacker overhearing the communications for a long period in parking lot). The analysis of the efectiveness of pseudonym change provided by (Beresford *et al.*, 2003), defining mix-zones to provide privacy in pervasive computing, has been exploited by different authors. In (Dötzer, 2005) the concept of short-term certificates with centrally assigned pseudonyms for VANETs was proposed. Authors define a system where vehicles change pseudonyms in a certain region pointed out by the system, the

[1] Pseudonyms are identifiers used by subjects to avoid the use of real information Pfitzmann & Hansen (2005).

region is defined when a large number of vehicles are within the communication range, a disadvantage appears when there are not enough vehicles changing pseudonyms within the region. In (Golle *et al.*, 2004) authors propose self assigned digital pseudonyms, taking a set of measures while changing them: *(i)* synchronizing pseudonym change, *(ii)* introducing gaps (silent periods) and *(iii)* changing pseudonyms when nodes are in the region (this was also considered in (Gerlach, 2006), by defining them as mix-contexts in addition to frequently change of pseudonyms and protection of a centralized mapping that intend to increase anonymity). CARAVAN (Sampigethaya *et al.*, 2005), also proposes a random silent period in order to hamper linkability between pseudonyms. An improvement of mix-contexts was presented by (Gerlach & Güttler, 2007), considering anonymity over randomly changing pseudonyms in certain intervals. In Choi *et al.* (2005) authors proposed a system to balance auditability and privacy in VANETs based on symmetric cryptographic primitives and two different sorts of pseudonyms (short and long term). A study of practicability in pseudonymity deployment and implementation is done in (Fonseca *et al.*, 2007), where possible solutions are represented as a combination of existing pseudonymity algorithms. Authors of (Liao & Li, 2009) proposed the synchronous pseudonym change algorithm where vehicular status information was taken into consideration and claimed to be more effective than those based on the mix-zones concept. However, even though pseudonym-based approaches are a commonly accepted solution to protect privacy in VANETs there are still open issues to be solved. Certificate revocation has then been identified as one of these important issues, mainly due to *i)* the large number of certificates to be issued for a single vehicle, and *ii)* the need of "fresh" revocation information, which has led to the need of implementing additional mechanisms.

3.3 Certificate Revocation

In common PKI approaches certificate revocation is assumed to be done with the distribution of CRLs which contain the most recently revoked certificates. However, CRLs can be very long due to the increased number of vehicles and

their high mobility, even short lifetime of certificates still creates a vulnerability window.

Authors of (Fischer *et al.*, 2006) proposed the SRAAC protocol which allows distribution of certificates, anonymous message authentication with quorum based blinded certificate issuance, anonymity, revocation and isolation of misbehaving vehicles. The protocol introduces a set of intermediate certification servers, previously certified by a CA. Making use of a digital signature algorithm called Magic Ink-DSS with shared secrets mainly provide revocable anonymity, where more than one entity must agree to be able to revoke anonymity. The main drawback of the proposed revocation model is that when a vehicle is detected as malicious, it cannot be immediately isolated because of the number of certificates previously stored in its On Board Unit (OBU), which will still be valid for some arbitrary time. A more complex approach was proposed by authors of (Papadimitratos *et al.*, 2008), which consisted of three different protocols: *(i)* Revocation using Compressed Certificate Revocation Lists (RC2RL), *(ii)* Revocation of the Tamper-Proof Device RTPD, and *(iii)* Distributed Revocation Protocol DRP, each one adapted to a specific VANET scenario. In the RC2RL and RTPD when revocation occurs the CA sends a message to the "revoked vehicle", however other relying parties (vehicles and service providers) do not receive this notifications, which opens a security gap on the whole VANET system. In the case of the DRP protocol, the possibility of collusion attacks remains open. Obviously the existence of an attacker detection system is assumed for the deployment of these protocols, has not yet been designed.

Authors of (Haas *et al.*, 2009) proposed a mechanism based on bloom filters, and consisting of two main mechanisms, one to reduce the size of the CRLs and the second one to organize and distribute the updates on the CRLs instead of the full CRL itself. However, the use of CRLs represents two major problems. First, is that static lists are difficult to handle, and second is that in distributed environments involving different CA domains, the management of trust relationships with CRLs could become cumbersome. In "traditional" PKI environments OCSP-based protocols have been proven to be a secure alternative to CRLs; however, in VANETs, this option has been discarded with the common argument that if communication failures occurred, the OCSP revocation information would be

hard to manage. Authors of (Papapanagiotou *et al.*, 2007), presented a certificate validation scheme based on a distributed version of OCSP for authorization and authentication in VANETs. Their approach focused on distributing cached OCSP responses, thus avoiding the exchange of extended certificate status lists. We believe this is an interesting approach that could be complementary to our contributed solution, to be further discussed in Chapter 4.

3.4 Group Signature

In order to reduce the number of exchanged keys in VANETs, the idea of group signatures emerged as an alternative to traditional PKI approaches. In a basic group signature scheme (Chaum & Heyst, 1991) participants are identified as follows:

- Group Leader: A trusted entity (vehicle or RSU) responsible for managing the group: initializing and handling joins and leaves (revocations). It is also responsible for de-anonymizing a signature in case of liability.
- Group Members: Vehicle representing current set of authorized signers. Each vehicle has a unique private key allowing it to sign on behalf of the group and a group public key.

Yet, a number of group signature schemes varying in assumptions, complexity and features have been proposed.

A mechanism for access control in VANET's network using the Kerberos model was described in (Moustafa *et al.*, 2006). The authors proposed an authentication and authorization mechanism to access offered services according to a previous subscription (token), so afterwards the vehicle is authenticated at the highways entry points, this model explored a hybrid approach where group signatures where considered as part of the solution. However, the proposed approach was specific for highways environments, thus limiting its applicability. Authors of (Guo *et al.*, 2007) introduced a group signature approach which, combined with role based access control vehicles were able to sign messages on behalf the group, thus achieving conditial anonynimity, that could only be reverse by the group leader. The

main disadvantage of this approach is that, group establishment is handled in a static way, where vehicles are pre-loaded with the corresponding group keys, and moreover, when traveling to different domains (geographical regions) vehicles must have in advanced the keys of all the groups belonging to the correspondiong hierachical regions. Following a similar idea, authors of (Lin *et al.*, 2007) presented a group-based approach where vehicles own a group signing keys issued by a trusted group leader. As an alternative to the aforementioned proposals, a hybrid approach has been presented by the authors of (Hui *et al.*, 2010). Their proposal consists of a combination of group-based signatures and identity based signatures, where the former are used for authentication among private vehicles and, the latter for public vehicles and RSUs. Nevertheless, the main drawbacks of group-based approaches include: *i)* that vehicles must trust a group leader that is responsible for issuing the corresponding signing keys; *ii)* due to the speed and trajectories of vehicles, group members should be considered volatile rather than permanent and, therefore, using a regular vehicle as a group leader might compromise the communications availability; *iii)* a large number of members in a group could increase the computational complexity, the total number of exchanged messages and thus severely impact the overall system performance and *iv)* interoperability issues have been considered only in a static form, which is not sufficient for a highly dynamic environment such as a VANET.

To overcome the trust issues originated due to the group leader being a regular vehicle, authors of (Xiaoping & Jia, 2012) present a new group-based certificate solution. The main difference among other group-based solutions is that in the latter, the group certificates are issued by the RSU's, which are assumed be trusted by following a top authority approach (however, note that RSUs are also considered vulnerable to different security attacks, and, therefore, can not be completely trusted).

3.5 Identity-based Cryptography

Non-PKI approaches have mostly focused in identity-based cryptography. The concept of identity-based cryptography was introduced by (Boneh & Franklin, 2003) to ease the deployment of the PKI by simplifying the management of a

large number of public keys. However, it is important to mention that it is based on an underlying public key cryptosystem and the issuance and utilization processes are very similar to those used in a traditional PKI domain. In VANETs, this idea was first adopted by authors of (Lin *et al.*, 2007), who proposed an approach based on group-based signatures (as discussed above), and this idea was followed by authors of (Mahmoud Al-Qutayri, 2010). However, their approach although interesting, lacks many implementation details, specifically on the certificate revocation process. Moreover, neither the interoperability issues among different domains nor the impact on performance are discussed.

3.6 Open Issues

Up to now, research proposals have envisioned a wide range of certification authorities (CAs) acting as trusted third parties within regional scopes, which in turn, result in the implementation of inter-domain authentication protocols and the establishment of trust issues among them (e.g. a German vehicle requesting services in a French infrastructure). However, the security implications derived from the VANETs' inter-PKI authentication process i.e. interoperability issues, have been mostly overlooked by the aforementioned research works by assuming explicit cross-certification agreements, which, in turn, are based on a static approach and have been proven to be hard to manage. In order to provide VANET interoperability among untrusted PKI domains, a PKI-based authentication protocol capable of dynamically establishing trust relationships among unknown domains is proposed and will be introduced in Chapter 4. Moreover, research proposals aiming to improve privacy, mainly focus on the use of pseudonyms, and algorithms for changing them in a more efficient form, however pseudonyms cannot prevent the automatic collection of information allowing an attacker to keep track of users and vehicles actions (e.g. behavior, movements, preferences, characteristics, etc.). Nevertheless, because of the common belief that pseudonyms are important for VANETs' overall security and are quite beneficial for protecting users' identity, a privacy compliant solution should be fully compatible with pseudonymity, a privacy-aware protocol based on attribute credentials will be introduced in Chapter 5. Finally, emerging schemes such as group signature,

although interesting, must deal with a set of open issues mostly associated to efficient and dynamic management of groups in terms of trust and communications overhead.

Chapter 4

Geolocation-based Trust

In a traditional non-VANET Public Key Infrastructure (Housley *et al.*, 1999), to validate and trust in an entity's certificate for Authentication and Authorization purposes, there should be a certificate path pointing to a trust anchor (root of trust of a certificate). However, in a VANET system, these anchors will change with the vehicle's location, as a result, this trust information needs to be propagated as soon as a driver joins a new geographical position, e.g. when traveling from Germany to France. Once the driver crosses the border, new authoritative PKI information should be sent just as shown in Figure 4.1. This chapter introduces the concepts of basic and extended path validation, towards proposing an security model, which specifically addresses the interoperability and revocation challenges derived from *v2v* and *v2i* communication scenarios, in particular, when a vehicle from a unknown domain is involved in the communication.

4.1 Introduction

Authentication protocols based on Public Key Infrastructure technologies (*PKI*) have proved useful for VANETs, mostly thanks to the several security features that these solutions offer. Take, for example, the use of encryption to query a VANET's service provider while avoiding eavesdropping. Also, the use of PKI and digital certificates enable the use of digital signatures, in order to provide more guarantees to, for example, exchange emergency messages among vehicles in the case of road accidents. Unfortunately, the sole implementation of PKI on

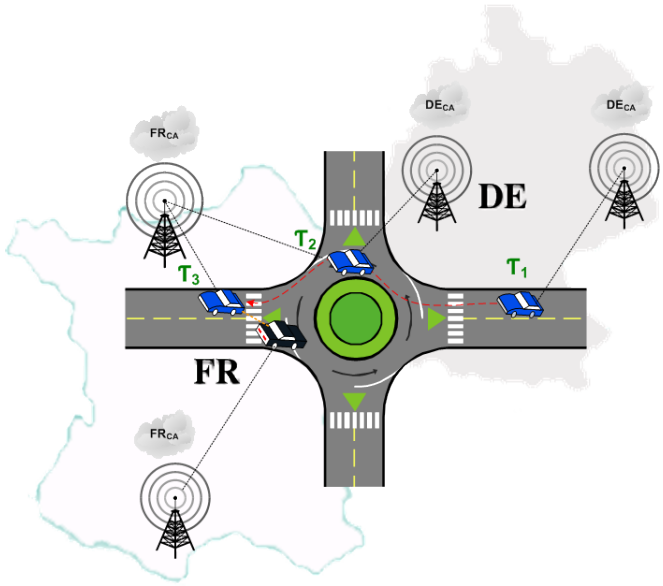

Figure 4.1: Geolocation-based Trust

a highly distributed environment such as in VANETs, comes with a important challenges:

- Lack of real-time revocation: considering the current version of the ITU-T X509.v3 standard (Housley *et al.*, 2002) only considers the use of Certificate Revocation Lists (CRLs). As it has been previously analyzed (Chapter 3), real-time information exchange is an important issue and the common CRL-based solution might not be appropriate to VANET environments, where in many cases, the different entities require "fresh" (updated) status information about the drivers' and vehicles' digital certificates. Moreover, alternative solutions such as OCSP also represent interesting challenges for VANET scenarios and must be carefully addressed, in particular with communication failures.

- Interoperability: as mentioned in Chapter 2, the use of several Certification Authorities (CAs) in VANETs conveys several interoperability challenges. The big question here is: how to assess the "trust level" of a CA, in order to decide if it is "trusted enough"?

- Privacy: Common PKI approaches are based on long-term certificates associated to a digital identity. Since PKI was not intended to overcome any privacy issues, thus personal information contained in certificates might not be properly used by third parties.

To provide interoperability among untrusted domains, existing approaches based their solution on static certificates and trust relationships among participants (Section 2.2), resulting in additional security considerations e.g. vehicles needing to access up-to-date CA's information in order to accurately validate messages received on the road. Analyzing the previous example of a German vehicle traveling to a different domain -France (Figure 4.1). While the German vehicle owns a certificate issued by the German CA, vehicles and the infrastructure in France will communicate with messages digitally signed by certificates issued by the French CA. Authentication among the involved vehicles and the infrastructure implies a certificate validation process that will include *i)* cryptographic verifications over the certificate path, *ii)* certificate's validity period verification, *iii)* certificate status verification, and *iv)* first certificate in chain verification. Based on this example, the main interoperability issue is **how can the validation process be performed if the trust anchor cannot be determined?**. Let us remember that the German CA is unknown to the French VANET infrastructure and vice versa. Also another question rises due to this trust issue: **how will the involved parties validate the revocation information?**. Next section introduces important concepts to provide a better understanding of the proposed model (further discussed in Section 4.4).

4.2 Concepts

To achieve validation and interoperability among untrusted VANETs PKI domains the proposed Inter-domain Authentication System for VANETs (further discussed in Section 4.5) is based on the Online Certificate Status Protocol (OCSP) standard (Myers *et al.*, 1999) which is by no means new, and has been successfully implemented in other distributed environments (Casola *et al.*, 2007c). In this section the basic concepts behind the proposed approach are introduced.

4.2.1 Basic Path Validation

According to the x.509 v3 standard (Housley *et al.*, 2002), the Basic Path Validation is the process that determines if a digital certificate is "trusted", according to the following criteria: *i)* the verifier has to verify the digital signature, *ii)* the information within the certificate (expiration date, certificate version, etc), *iii)* the suspension/revocation status and *iv)* the validity of all certificates in the certification path until a trust anchor. It is easy to observe that the "basic path validation" process does not include any check to assess the trust level of the issuing CA, and even more importantly, does not perform any real-time lookup on the certificate's status, thus opening a vulnerability window for the whole system. To complete the Basic Path Validation process, our proposal introduces the notion of near-real time validation via the Online Certificate Status Protocol OCSP (Myers *et al.*, 1999).

4.2.2 Multi-CA OCSP

OCSP, was created to be used instead of or as in most cases- in conjunction with other mechanisms like local Certificate Revocation Lists (CRL), to provide timely information regarding the revocation status of a digital certificate. Even though it was initially designed for applications carrying highly sensitive and valuable information, nowadays it is being used in a wide variety of systems.

When deploying a PKI, certificate validation using OCSP may be preferred over the use of CRLs for several reasons:

- OCSP can provide more timely information regarding the revocation status of a certificate.
- OCSP removes the need for clients to retrieve the (sometimes very large) CRLs themselves, leading to less network traffic and better bandwidth management.
- To a degree, OCSP supports trusted chaining of OCSP Requests between Responders. This allows clients to communicate with a trusted Responder to query an alternate Responder, saving client-side complexity.

OCSP is based on a request-response scheme, in which an OCSP Client issues a certificate status query to an OCSP Responder which includes the following data:

- Target certificate identifier, consisting of an unordered list of certificate identifiers formed with the issuer's distinguish name hash, issuer's public key hash and finally the serial number of the certificate whose status is being requested.
- Optional extensions which may be processed by the OCSP Responder; for example, to demand information about the Certificate Authority quality.

The OCSP request itself may be secured if the client uses a nonce (protection against replay attacks) and digitally signs it. Once received by the OCSP Responder, this request is verified (i.e. digital signature), processed and a definitive response message is produced. For each one of the certificates in an OCSP Request, the OCSP Response message will contain any of the following status: Good, Revoked (either permanently or temporarily) and Unknown. The signing key of the OCSP Responder is a very sensitive issue in a PKI environment and, in fact, depending on the certificate being used to sign the responses, we can define three different operation modes:

- Authorized OCSP Responder mode
- Transponder OCSP Responder mode
- Trusted OCSP Responder mode

For the proposal presented in this chapter, the "Trusted mode" in Figure 4.2 will be used to centrally provide a single OCSP service connected to several VANETs' PKI hierarchies. In Figure 4.2 it can be observed that the OCSP signing certificate (*subject* T) belongs to a hierarchy that differs from that of the certificates being requested (neither of A, Y or W). For example, the OCSP service has to be explicitly trusted by the user with subject X-. In practice, OCSP Responders working under such centralized models, implement a response cache (the "OCSP cache" from Figure 4.2) to increase their performance while reducing the number of queries to external Authorized OCSP Responders and other revocation sources (like CRLs through HTTP).

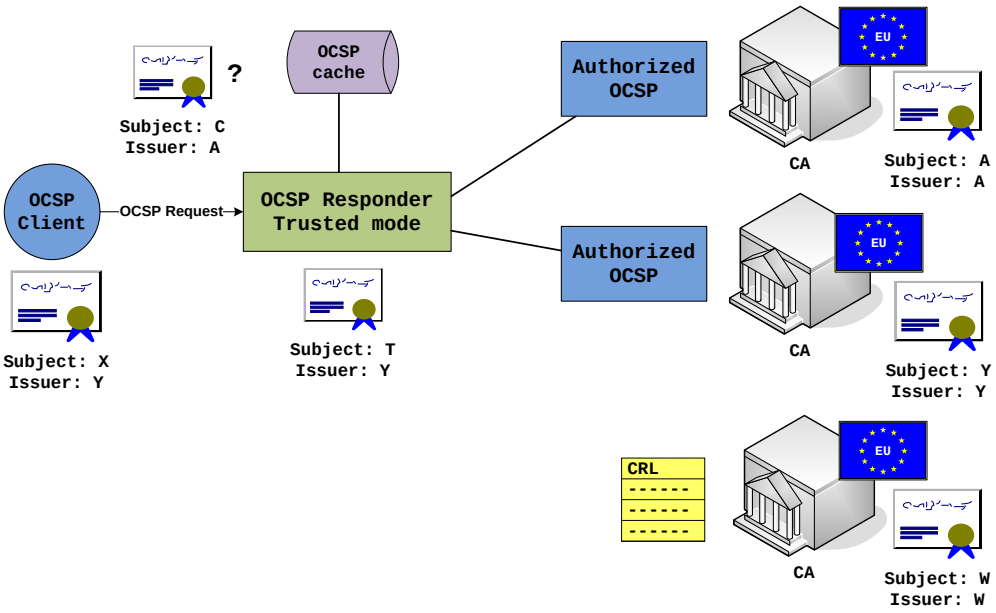

Figure 4.2: OSCP in trusted mode

4.2.3 Extended Path Validation

The methodology used to evaluate the security level provided by a Certification Authority and decide to create a dynamic trust relationship with it, is the Reference Evaluation Model (REM) (Casola *et al.*, 2007b). Its main goal is to provide an automatic mean to state the security level provided by an infrastructure; REM has been widely adopted in the past to dynamically build CA Federations.

4.2.3.1 CA Federation

In a CA Federation the members agree on a minimum set of security requirements that must be fulfilled by all of them to interoperate. These minimum requirements are usually a subset of the CA's Certificate Policy (CP) and can be audited at any time by the other members of the same Federation. If a new CA wants to participate in the Federation, then its CP must pass through an "accreditation" process to ensure compliance with the minimum requirements or, in other case, to assess the candidate in which provisions (individual rules from the CP) should be improved to become a member. Once the accreditation process has been

passed the new member CA's root certificate is added to a trusted repository (usually hosted by the Federation itself). Instead of distributing new sets of cross-certificates to all the VANET's nodes it is only necessary to let them know how to access the CA Federation's repository in order to update their local copies of trusted CAs.

4.2.3.2 Reference Evaluation Model

The methodology REM basically defines *i)* how to express in a rigorous way a security policy (a Certification Policy in our particular case), *ii)* how to evaluate a formalized policy and, *iii)* how to state the provided security level. With REM any policy is represented through an XML tree containing all its provisions as intermediate nodes and leaves.

1. The **Structuring phase** associates an enumerative and ordered data type K_i to the n leave-provisions of the policy. A policy space *"P"* is defined as $P = K_1 \times K_2 \times ... \times K_n$, i.e. the vectorial product of the n provisions K_i. For example, the provision *KeyLenght* can assume the following ordered values: {*128bits, 512bits, 1024bits, 2048bits*}. The space is defined according to a policy template that strongly depends on the application context.

2. The **Formalization phase** turns the policy space "P" into an homogeneous space "PS". This transformation is accomplished by a normalization and clusterization process which allows to associate a Local Security Level (LSL) to each provision. For example if a policy has a *KeyLenght* of 512$bits$, it will be associated to the $LSL = 2$ and the normalized vector is $(1, 1, 0, 0)$. After that the provisions may be compared by comparing their LSLs.

3. The Evaluation phase pre-processes the "PS" vector of LSLs in order to represent it by a $n \times 4$ matrix whose rows are the single provisions K_i and the number of columns is the chosen number of LSLs for each provision. For example, if the number of LSL is four and the LSL associated to a provision is l_2, the row in the matrix associated to the provision in the matrix will be: $(1, 1, 0, 0)$. Finally, a distance criteria for the definition of a metric space is applied. REM adopts the Euclidean distance among matrices:

$d(A,B) = \sqrt{(\sigma(A-B, A-B))}$
where $\sigma(A-B, A-B) = Trace\ ((A-B)(B-A)^T)$

In summary, REM's goal is to evaluate the GSL or security level associated with a CA through the evaluation of its Certificate Policy so trust decisions can be taken. To better illustrate our proposal and how the aforementioned concepts can be effectively adopted by VANETs the two basic communication scenarios will be presented, mainly consisting of the interactions performed in v2v and v2i communications.

4.3 Authentication Requirements in VANETs Communications

Following the communication model presented in Chapter 2, this section analyzes different scenarios where authentication is required and how should be achieved, in particular highlights the challenges that are present in typical situations of the v2v and v2i communication.

4.3.1 Vehicle to Vehicle Authentication

This scenario includes v2v communication without infrastructure availability, considering that, in a VANET environment vehicles need to authenticate each other in different situations that are classified according to the following:

- A vehicle offering a "service" is a good example in terms of information sharing (personal o related to a particular service). Before granting any kind of permission the vehicle offering the service needs to validate the requestor's vehicle credentials.
- A vehicle receives a message from other vehicle (e.g. a safety related message), and therefore needs to "prove" the message's legitimacy by validating the sender's credential.

Both situations require a local authentication service able to address two main issues: *i)* how to provide local authentication if the infrastructure is unavailable?, and *ii)* how to deal with a situation where vehicles belong to different domains?

4.3.2 Vehicle to Infrastructure Authentication

This scenario involves vehicle-to-infrastructure communication, where vehicles communicate with the RSUs available on the roads. The infrastructure is able of providing different kinds of information that are strictly dependent on the vehicle's requests and geolocation, and that can be classified into the following situations:

- A vehicle needs to access a location-based service or any other service offered by a Service Provider (SP). Before granting access and providing the requested information the SP must validate the vehicle's credentials.
- A vehicle receives a message from the infrastructure (e.g. a safety related message, service response), and therefore needs to "prove" the message's legitimacy by validating the sender's credential.
- In a v2v communication where vehicles need to authenticate each other, and in the case of infrastructure availability then the vehicles request trusted information from the infrastructure in order to mutually validate their credentials.

All situations include the use of authentication services, which are actually provided by the infrastructure and that must deal with the issue of interoperability among different CAs. The main security issues to be addressed in this scenario are: *i)* how can a vehicle implement interoperable and secure authentication in VANETs?, *ii)* how to allow vehicles in a VANET to perform authentication under different (untrusted) domains?, and *iii)* how to deal with the communication failures that are inherent to the VANETs system?

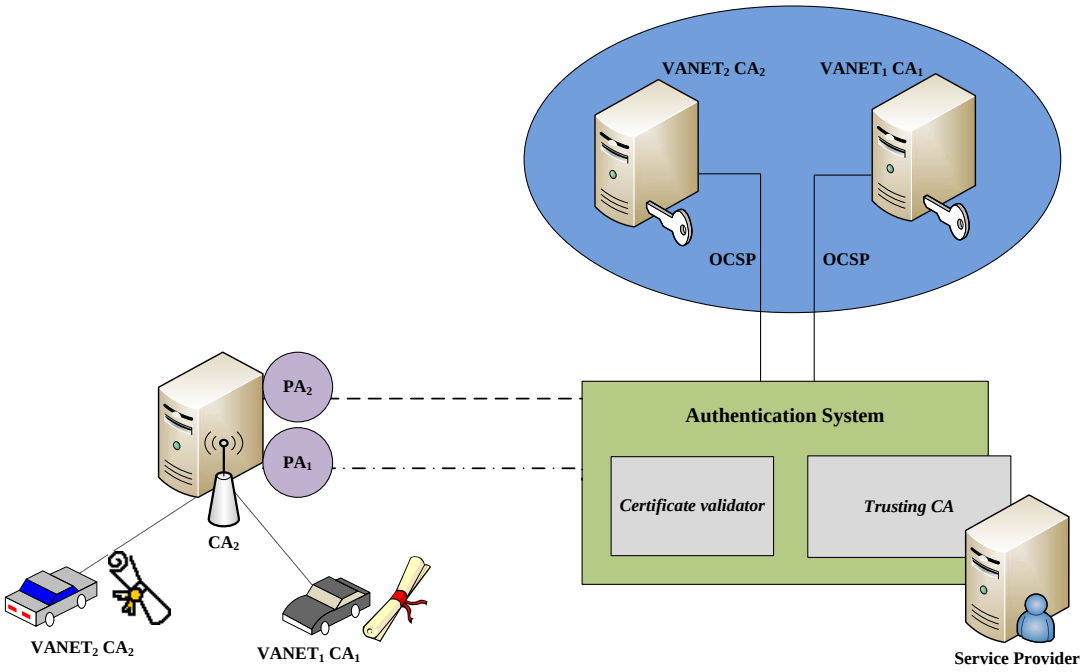

Figure 4.3: Security Architectural Model

4.4 Security Model for VANETs' Communication

The security analysis of the aforementioned scenarios lead us to model the VANET as two different networks: an ad hoc network of vehicles comprised of unreliable and dynamic connections (v2v), and a fixed network's infrastructure offering different services to vehicles (v2i). The v2i scenario models the communication between these two networks, while the v2v scenario represents an ad hoc communication. To face the issues presented by the previous scenarios, the VANET protocol should implement optimized messages where security (e.g. digital signature mechanism and cryptosystem being used) and performance (e.g. signature size and encryption time) are balanced. The security model proposed takes into account the overall VANET's security and performance requirements independently from the (proprietary) involved technology. At the design level, the security architectural model can be represented as in Figure 4.3.

Figure 4.3 depicts the main components of the proposed security model and shows that a VANET can be simply modeled as a distributed system composed by *i)* wireless communications among vehicles and RSUs, and *ii)* fixed communications among the RSUs, the Authentication System (AS), and a set of SPs hosting VANET's services. Note that vehicles belonging to different domains also own certificates issued by different CAs. The creation of several PKIs each one installing its own CA and thus giving birth to a large set of different and untrusted security domains, represents one of the biggest interoperability and security problems that could arise among all VANET users.

The security model proposed in this thesis faces this problem with the adoption of an Authentication System, that acts as an intermediary between the certificate verifiers (vehicles and service providers) and the issuing CAs by means of two validation mechanisms (namely basic and extended path validation)(Sections 4.2.1 and 4.2.3, respectively). The details of the proposed Authentication System will be further discussed in Section 4.5. On the other hand, the proposed model also faces the problems originated due to the inherent connectivity failures by associating a Personal Agent (*PA*) to each vehicle's request. The PA acts on behalf of the vehicle that generated a service request by means of a delegation model: the vehicle's PA activates and interacts with the Authentication System in the "wired" network, while keeping the vehicle's session status. In other words, when a vehicle needs to deal with connection failures (e.g. if for any reason loses connection before receiving the requested information from the infrastructure), then its associated PA will be capable of maintaining the last connection status. As soon as the vehicle reconnects to the infrastructure, its PA will send the corresponding request result. Further details on the different protocols used in the proposed security model will be discussed in Section 4.6.

4.5 Inter-domain Authentication System

In order to contribute to a solution for the aforementioned scenarios (Section 4.3), and taking into account the unique features of a VANET, the authentication system proposed in Section 4.4 contains a set of basic functionalities that allow:

1. The use of near real-time revocation information for multi-CA VANET environments, based on the OCSP protocol.

2. The use of a security metric able to compute the "security level" associated with a digital certificate, also in near-real time, in order to decide if the VANET nodes should trust it or not.

The main goal of the Authentication System (AS) is to enable the basic and extended path validation of digital certificates. According to the x.509 v3 standard, the validation of a digital certificate issued by any CA, may consist of two different set of operations:

1. if the CA is trusted, the verifier has to verify the digital signature, the information within the certificate (expiration date, certificate version, etc), the suspension/revocation status, the validity of all certificates in the certification path until a trust Anchor — basic path validation — Section 4.2.1

2. if the CA is not trusted, the verifier has to perform the same actions as in point (1) and additionally has to evaluate if a trust relationship can be created with the otherwise untrusted CA. This action can be performed in a static or dynamic way — extended path validation — Section 4.2.3

While the first point is widely adopted in the literature and implemented in many available applications, the second point is more delicate. At the state of the art, only static extended path validation is performed and implemented in real world applications. It is primarily based on extending trust links to an untrusted CA by explicit human-based agreements that result in cross-certification processes and, the issuance of cross-certificates that the relying party can use as Trust-Anchors. Nevertheless, the techniques to dynamically extend trust are promising and some scientific works have appeared in the literature (Casola *et al.*, 2007c) to adopt innovative CA evaluation metrics towards this goal. To perform validation operations (both basic and extended), the proposed Authentication System is made of two main components: a Certificate Validator and a Trusting CA component, as illustrated in Figure 4.4. The Certificate Validator is in charge of providing near-real time certificate's status information; while the

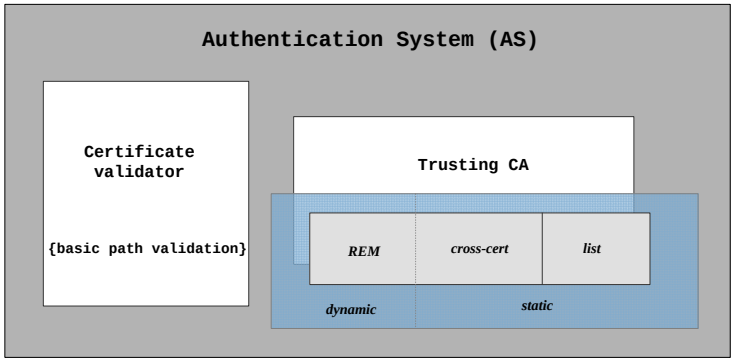

Figure 4.4: Authentication System Components

Trusting CA component establishes a trust level across unknown domains. In the following subsections, the main details of these two components will be described.

4.5.1 Certificate Validator

This module is in charge of improving the so-called Basic Path Validation process (introduced in Section 4.2.1) via the use of near real-time certificate validation. The primary goal of a Basic Path Validation process is to verify the binding between a subject's distinguished name or a subject's alternative name and the subject's public key -as represented in the end entity certificate-, based on the public key of the trust anchor (i.e. a Certification Authority). This process requires obtaining a sequence of certificates that support that binding. To meet this goal, the path validation process verifies, among other things, that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

- For all x in $\{1, ..., n-1\}$, the subject of certificate x is the issuer of certificate $x + 1$;
- certificate 1 is issued by the trust anchor;
- certificate n is the certificate to be validated; and
- for all x in $\{1, ..., n\}$, the certificate was valid at the time in question.

As mentioned before, the Certificate Validator by itself cannot decide the trust level of the issuing CA or the real-time revocation status of the digital certificate under evaluation. These are the reasons why the "Trusting CA" subsystem is proposed and will be introduced next.

4.5.2 Trusting CA

The Trusting CA component aims to evaluate the trust level associated with each one of the participating CAs via two different approaches: the static trust evaluation and the dynamic trust evaluation.

The static approach is based on off-line agreements between the CAs participating in a VANET environment. Usually these are bi-lateral agreements, meaning that if CA_1 trusts in CA_2, then the opposite is also true. Static trust's agreements are built using lists of trusted CAs or cross-certification processes. It is easy to notice that both approaches are cumbersome to maintain, therefore our proposal of using the dynamic trust evaluation approach, just as presented next.

The dynamic trust evaluation has been proposed in order to overcome the potential disadvantages of the static trust evaluation in ad-hoc environments, like e.g. VANETs. Taking into account the constantly changing trust relationships among the CAs in a VANET, the belief is that, it is necessary to use techniques able to compute "on-the-fly" the trust level associated to each one of them. In order to do this, the Trusting CA subsystem implements two mechanisms. For evaluating the CA's security level and generating the dynamic trust relationship, the implementation of the Reference Evaluation Methodology REM- (Casola *et al.*, 2007b) is proposed, whose main goal is to provide an automatic mean to compute the security level of a digital certificate. This methodology has been widely adopted to dynamically build CA federations (Casola *et al.*, 2007a) and to complete the Basic Path Validation process, the Trusting CA introduces the notion of near-real time validation, a second core component namely the Online Certificate Status Protocol OCSP (introduced in Section 4.2.2), which is implemented as an interface between the Authentication System and the Multi-CA OCSP. OCSP was created to be used instead of or as in most of the cases- in conjunction with other mechanisms like local CRLs to provide timely information regarding the

revocation status of a digital certificate. Section 4.6 will describe the associated protocols of an interoperability system for VANETs.

4.6 Managing Interoperability Among Untrusted PKI Domains

The authentication system allows interoperable authentication in any distributed infrastructure, nonetheless the successful implementation of the AS must deal with the communication failures that are inherent for the VANET system due to its dynamic nature (infrastructure-less scenarios and nodes mobility). Consider a scenario where a vehicle moves from one RSU to another, where RSUs are positioned with a great distance in between, if the communication between the vehicle and the RSU is lost then keeping the request status and the secure management of messages are important challenges. In other words when a vehicle reaches the communication range from the second RSU, this new RSU must be able to provide the requested service. Dealing with communication failures is an important issue that is addressed by the AS by assuming that the communication among vehicles and infrastructure (v2i) is asynchronous, and a PA is associated to each vehicle. Within a VANET system both v2i and v2v scenarios can be represented by a combination of different parameters and the corresponding authentication protocol must cope with the particularities introduced by them:

- v2v communication takes place among two vehicles belonging to different domains. This scenario implies 2 different actions: *i)* a registration process (a vehicle asks for a temporary certificate through the infrastructure - AS and the OCSP responder), *ii)* a vehicle already owns a temporary certificate and can implement basic or extended path validation (locally or with the infrastructure).

- v2i communication takes place among vehicle and a Service Provider (SP), and the latter is in charge of validating the local or foreign credentials via the AS.

- v2v communication takes place among two vehicles belonging to the same trusted domain and i) there is no infrastructure availability to validate credentials, therefore the basic path validation (Section 4.2.1) must be implemented or ii) there is infrastructure availability to validate credentials, so in this case the extended path validation can be implemented (Section 4.2.3).

4.6.1 Extended v2i Communication Protocol

As mentioned in Section 2.2, a vehicle in a VANET will own a certificate issued by its regional Certification Authority (CA), which allows inter-vehicle or vehicle to infrastructure authentication. Within a region, credentials will be validated by simply performing the basic path validation. In order to communicate with vehicles or infrastructure in a different "untrusted" domain (e.g. a different country), vehicles are required to first perform a registration process in the new domain, so a new temporary certificate will be issued by the foreign Certification Authority. The temporary certificate will be validated locally by any other vehicle within the same domain, even if no infrastructure is available. Note that, if the vehicle does not own the temporary certificate; in order to be authenticated the extended path validation must be performed. This process will require a specific set of services from the infrastructure just as shown in Figure 4.5, where a combination of synchronous and asynchronous communication takes place in order to:

1. Authenticate a vehicle to provide infrastructural services
2. Authenticate a vehicle with extended path validation.

An alternative to include the full digital certificate in the proposed protocol is to use a unique identification for it (let us call it $Cert_{ID}$). This is the design has been decided to follow, because as will be seen in Chapter 7, the use of a $Cert_{ID}$ dramatically reduces the size of the exchanged messages. The $Cert_{ID}$ can be build via an approach like the one used by RCF 2560 ((Myers *et al.*, 1999)), and just as shown in Table 4.1

Where:

Cert_id ::=	SEQUENCE { hashAlgorithm AlgorithmIdentifier, issuerNameHash OCTET STRING, – Hash of Issuer's DN issuerKeyHash OCTET STRING, – Hash of Issuers public key serialNumber CertificateSerialNumber }

Table 4.1: OCSP's Certificate ID structure in ASN.1

- issuerNameHash is the hash of the Issuer CA's distinguished name.
- issuerKeyHash is the hash of the Issuer CA's public key.
- The hash algorithm used for both these hashes, is identified in hashAlgorithm.
- And serialNumber is the serial number of the vehicle's certificate for which the status is being requested.

As shown in Figure 4.5, for the implementation of the asynchronous protocol the proposed approach is based on a set of PAs that are able to store a session's requests in order to maintain its state - especially when connections are lost -. Figure 4.5, also shows that the RSU receives a vehicle's signed requests towards a specific service (e.g. registration, validation or any other service offered by the infrastructure). The RSU's server creates a PA and associates the corresponding request to it. Afterwards the identification of the Personal Agent (PA_{ID}) is sent to the vehicle as an acknowledgement. In turn, the PA acts on behalf the vehicle within the infrastructure in order to complete the authentication process through performing the extended path validation and forwarding the vehicle's request to the SP after successful authentication. Finally the PA will store the results of the original request, to be forwarded to the requestor (vehicle), even if the connection was lost. In subsequent messages, vehicles will include their PA_{ID}, which can be verified by the VANET infrastructure in order to return the previously stored results. Note that the proposed protocol was designed taking into consideration the connection constraints of a VANET (only a few messages must be exchanged), and by adopting an asynchronous approach (messages being

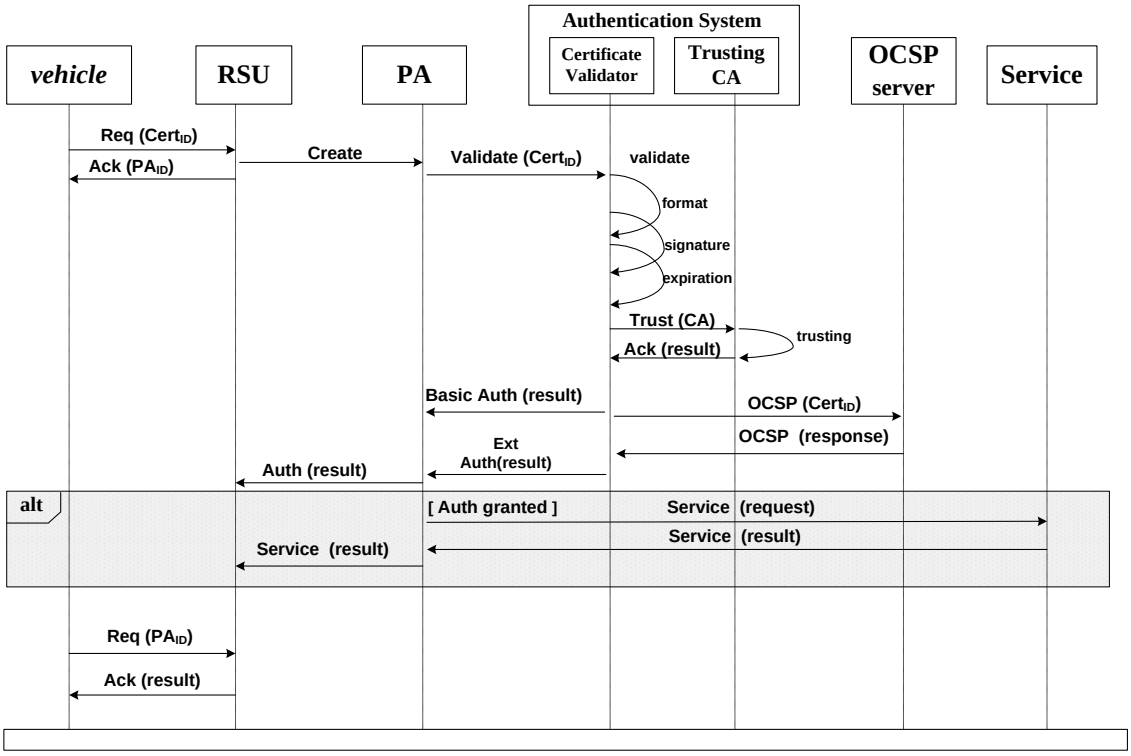

Figure 4.5: v2i Communication Protocol

exchanged are short and do not require any complex behavior). In fact, it is the Personal Agent residing on the RSU server and communicating with other components within the VANET's fixed network, the one in charge of managing the complex elaborations. Thus in this case, security is granted due to the certificate delegation model between the vehicle and the PA. By following the asynchronous approach just described, if the client sends a request before the result is available, then the server will then return a "Null" message.

4.6.2 Extended v2v Communication Protocol

This protocol is aimed at providing local certificate validation (basic path validation) in v2v communications. The underlying mechanisms have been specifically designed to deal with the infrastructure unavailability. Just as depicted in Figure 4.6 when vehicle1 requests information, it sends a signed message to $vehicle_2$, which in turn generates a req_{id} that is sent back as an acknowledgement. In order to perform the basic path validation without infrastructure availability, $vehicle_2$ must have stored "cached" the Public key of the issuing CA. Additionally, in order to enforce the local certificate validation, our proposal assumes that vehicles will also be capable of storing a list of previously validated certificate identifiers (validated through the infrastructure). This list will be stored for a temporary period of time t, thus enabling vehicles to determine whether certain credentials were successfully validated before, similar to CRL distributions mechanisms discussed in Section 3.3, this approach also supports distribution of cached OCSP responses. Going back to 4.6 $vehicle_2$ will then locally validate credentials of $vehicle_1$, and as in the previous protocol for subsequent messages of the session, $vehicle_1$ will attach the req_id in order to gather the requested information from $vehicle_2$.

Note that in infrastructure-less scenarios, even with the use of the list of previously validated credentials and OCSP cached responses, there will exist a vulnerability window that cannot be prevented (e.g. certificates that have been recently revoked will still appear to be valid), however other mechanisms can be used to reduce this risk such as local validation of messages according to

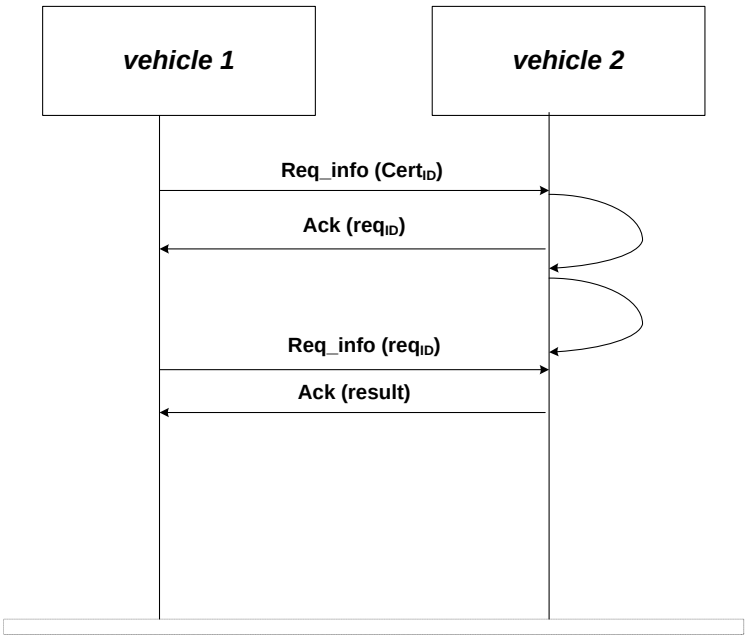

Figure 4.6: v2v without infrastructure - basic path validation

its classification. Let us take for example the setting of different priority levels according to the message types (e.g. warning message priority level 1, weather conditions priority level 2, etc), by assigning "trust" levels referencing the type of vehicle in the VANET (e.g. ambulance trust level 1, police car trust level 2, etc). With the combination of these two strategies, the aforementioned risk could be severely reduced. The exploration of these additional strategies will be further discussed in Chapter 6.

4.6.3 Enabling Vehicular Communication in Untrusted Domains

To enable communication among untrusted domains, a vehicle (vehicle1) with a certificate issued by its local CA ($Cert_CA1$) must first perform a registration process in order to gather a temporary certificate from the foreign CA (CA2). This registration process can be defined as follows.

1. A vehicle entering a new domain authenticates to the infrastructure via a

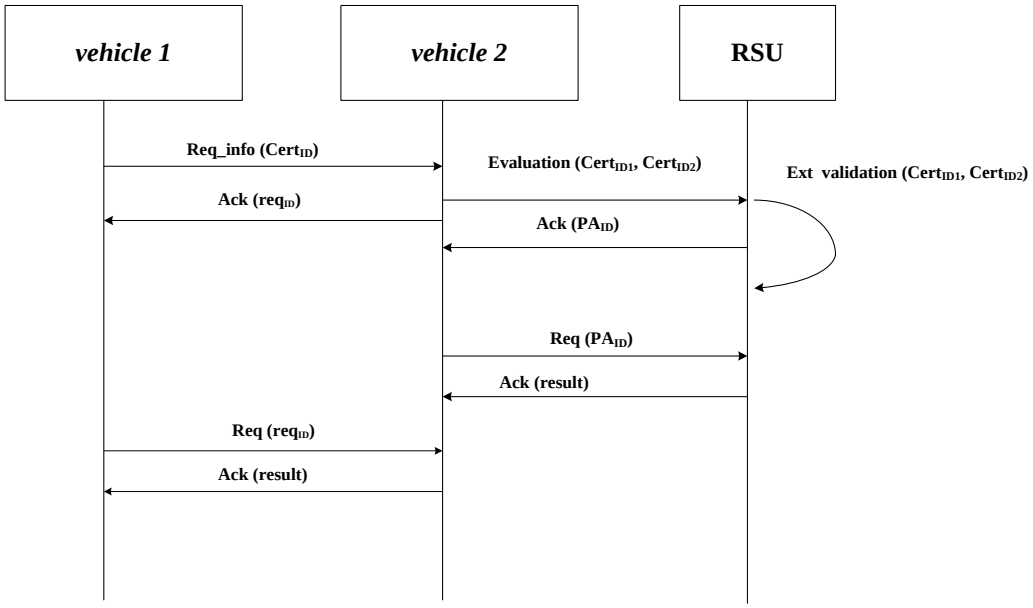

Figure 4.7: v2v with infrastructure availability - extended path validation

RSU (this implies v2i communication just as described in Section 4.6.1 and Figure 4.5).

2. The RSU requests to the local CA authority the issuing of a temporary certificate

3. The CA authority validates the current certificate, extends trust, registers the user in its directories and issues the new temporary certificate that is delivered to the vehicle via the RSU.

Once the registration process has been successful; a vehicle can authenticate another vehicle in both basic and extended modes. In particular if the infrastructure is not available, then the protocol described in Section 4.6.2 and Figure 4.6 must be performed. If the infrastructure is available then the extended path validation is possible, just as shown in Figure 4.7.

Figure 4.7 represents the communication flow involving the following scenarios:

1. v2v communication between two vehicles belonging to untrusted domains: this scenario might involve a previous registration process where the foreign vehicle will own a temporary certificate issued by the local CA, and this registration process will simplify further validation interactions. Within this process the infrastructure will perform validation and authentication process via the OCSP responder in order to gather certificate information from the issuing CA. Note that without the registration process and considering infrastructure availability it is still possible to perform the same validation process via OCSP, however the main advantage of the temporary certificate is to reduce the number of executions of the whole process and ease the interactions among vehicles when no infrastructure is available (local validation of certificates issued by the same CA).

2. v2v communication belonging to the same domain: considering the infrastructure availability this scenario will involve the implementation of the extended path validation for certificates issued by the same CA.

The interactions in the v2v communications are shown in Figure 4.7 and explained next. First, $vehicle_1$ sends a message to $vehicle_2$; this message will include its own certificate identifier ($Cert_{ID1}$). Then, $vehicle_2$ replies with a req_{ID} as an acknowledgment to $vehicle_1$*'s* request. Afterwards, in order to perform the extended path validation, $vehicle_2$ sends to the infrastructure (via RSU) a message including both certificate identifiers ($Cert_{ID1}$ and $Cert_{ID2}$). Just as described in the v2i protocol (Figure 4.5), the RSU generates a *PA* associated to *vehicle2's* request and sends the PA_{ID} as an acknowledgement. The PA acts on behalf $vehicle_2$ and performs all actions described in the v2i protocol. The *PA* stores the result that will be consulted by $vehicle_2$ within subsequent messages in the session. To validate whether the messages belong to previously established session the PA_{ID} must be included. Once $vehicle_2$ has the validation result from the infrastructure is then able to provide the results to $vehicle_1$ in subsequent messages of the session that will include the req_{ID}.

4.7 Open Issues

In this chapter an authentication system able to provide authentication among vehicles belonging to a different domain has been proposed, the AS is based on two main components, a OCSP based component that provided online status verification of a given certificate and a REM based component to build dynamic CA federations and establish dynamic trust relationships, since the introduced concepts rely on the infrastructure availability, a PA was also introduced to deal with the communication failures that are inherent to a VANET system. Nevertheless, two main open issues could be identified, *i)* the propose AS does not provide any privacy protection and *ii)* in scenario where the infrastructure is not available at all the local validation of certificate implies a security vulnerability window. To address the aforementioned privacy issues, the following Chapter introduces a privacy enhancing protocol based on the implementation of attribute credentials which in turn could be implemented on the PKI-OCSP based solution just described, finally the to be able to reduce the security vulnerability window on infrastructure-less scenarios, a policy evaluation mechanism will be introduced in Chapter 6.

Chapter 5

Enhancing Privacy in Vehicular Communications

This chapter presents a Privacy Enhancing Model which introduces the concept of Attribute Based Credentials (ABCs) to provide conditional anonymity. An overview of important concepts regarding ABCs will be introduced, followed by the description of the Attribute-Based Privacy model and its main architectural components. Additionally, the Anonymous Information Retrieval (AIR) privacy protocol based on query permutation and forgery aimed at alleviating user profiling in v2i communications will be described.

5.1 Attribute-Based Privacy

In typical PKI approaches, the use of certificates leads to unnecessarily revealing the identity of its holder, moreover, as previously discussed, PKI does not guarantee any privacy protection. In VANETs communications, when a driver or vehicle requests information to any other entity, the corresponding entity only needs to verify if the vehicle is authorized to access the requested resource or service, and does not necessarily needs to learn the corresponding identity. Revealing more information than necessary could lead to potential privacy risks. An attacker hearing the communications might be able to trace and link communications and transactions of each vehicle, in particular, in those scenarios where there are not enough vehicles communicating. The passive collection of information will enable

the attacker to keep track of driver's/vehicle's actions (e.g. behavior, movements, preferences, characteristics, etc.).

To overcome the aforementioned privacy issues, next section introduces basic concepts of Privacy Attribute-Based Credentials (P-ABCs) towards proposing an Attribute-Based Privacy (ABP) protocol for VANETs, that will effectively implement P-ABCs specifically to provide conditional anonymity and minimal information disclosure.

5.1.1 Privacy Attribute-Based Credentials (P-ABCs)

P-ABCs, are basically a PKI with privacy enhancing features. P-ABCs are issued just like ordinary cryptographic credentials (e.g. X.509 credentials) using a digital (secret) signature key (Camenisch *et al.*, 2012).

However, the main enhancing feature in P-ABCs, is that, credential's attributes could be transformed into 'unlinkable' presentation tokens able to protect the holder's privacy, and verifiable in a similar form, just like cryptographic credentials (using the public verification key of the issuer), and that offer the same strong security. Next section will introduce the main components in P-ABCs.

5.1.1.1 Components

This section describes the different entities involved in P-ABCs and how do they interact with each other.

User in P-ABCs the user is the entity to which the credentials are issued, and responsible for managing and selecting from which credential, which attributes will be disclosed and to which entities.

Attribute Authority (AA) the AA is responsible for issuing credentials.

Verifier the verifier is an entity willing to protect access to a resource or service, and is the one defining the attributes that a user must prove for the access to be granted.

Revocation Authority (RA) the RA is responsible for revoking issued credentials, in a form that these credentials will not be able to generate presentation tokens.

Inspector a trusted authority able to de-anonymize presentation tokens under specific circumstances.

5.1.1.2 Features

This section presents a high level description of the main functionalities offered by the P-ABCs. A more technical explanation can be found in (Camenisch *et al.*, 2012).

Credential issuance At initial stage, the AA generates public issuer parameters and a secret issuance key (similar to public key). The issuer parameters are used by verifiers to verify the authenticity of presentation tokens, and to create presentation tokens

Token generation The presentation token is derived from one or more credentials

Token presentation Tokens are sent to verifiers to provide certified information to from any number of credentials. The token can reveal a subset of the attribute values in the credentials or prove that one or more values satisfy a certain predicate. Presentation tokens support the use of pseudonyms.

Presentation Policy The presentation policies are published by the verifiers, and determine the conditions the must be met to access a resources or service, which credentials/issuers does the verifier trust, and which information should the token reveal or prove.

Token inspection Token inspection is a form to somehow reverse anonymity, conditional anonymity is provided only if token were generated in compliant with a presentation policy that specifies the information that should be recoverable by an inspector.

De-anonymization Is the result from the token inspection, typical example is related to liability, however, other scenarios include that for certain service, the SP might rely in a Trusted Third Party (TTP) for example for payments, the SP will publish in the presentation policy which information should be encrypted using the TTP public key.

5.1.2 Attribute-Based Privacy (ABP) Protocol

In VANETs the implementation of a VPKI with hierachical certification authorities is envisioned. In Chapter 4, an AS able to provide PKI-based authentication among untrusted domains was introduced. However, although the proposed approach copes with interesting challenges, privacy issues remain unsolved. Thus additional mechanisms to support conditional privacy must be considered as an integration of the underlying solution. This section describes the proposed PKI-compliant ABP protocol, which inspired by P-ABCs implements conditional privacy, specifically to address vehicle's tracking (big brother scenario). Next section describes the main component of the ABP.

5.1.2.1 Entity's Definition

In compliance with the VPKI and P-ABCs, as shown in Figure 5.1, the ABP defines three different types of entities the will be introduced next.

Attribute Authority (AA) the AA is the authority responsible for issuing and revoking the corresponding attribute credentials. In VANET scenarios the AA could be represented by the regional CA or by any trusted authority in charge of issuing, revoking, and when applicable revealing the attribute-based credentials. Note that ABCs are different than the short-term credentials issued by the AS.

Vehicle/Driver in ABP, entities to which the AA will issue the ABCs, will be mainly represented by vehicles and drivers. This entities will be responsible for managing and selecting from which credentials, which attributes will be disclosed and to which entities, and ultimately will be responsible for generating a presenting the corresponding presentation tokens.

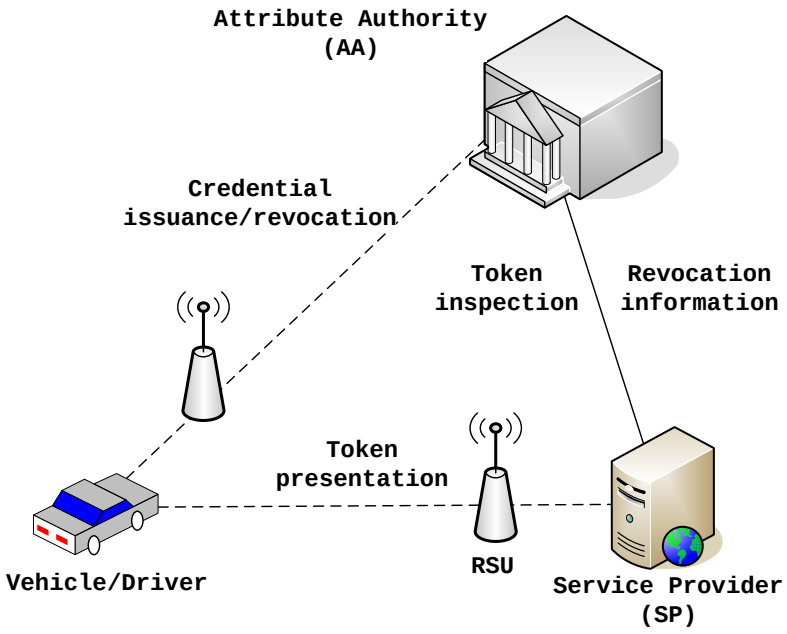

Figure 5.1: ABP protocol involved entities

Service Provider (SP) The SP consists of any relying party willing to protect access to resources, information or services, in common VANET scenarios the SP could be represented by RSUs, vehicles, authorities, or services provided by the infrastructure. In VANETs SPs will define the attributes and conditions that should be included in the presentation tokens for vehicles and drivers to prove, and, the access to be granted.

The implementation of the ABPs in VANET relies on the existence of the PKI-based AS. That is, since ABP strongly depends on the AS, it is very likely that the AA will actually be represented by the same CA responsible for issuing certificates in VANET. The process to obtain the attribute credentials will be described next.

5.1.2.2 Credentials Issuance

By implementing the AS, the credential issuance process assumes that a vehicle in a VANET posses a certificate issued by a trusted CA. At initial stage, upon request, the vehicle will provide either the $Cert_{ID}$ or the full certificate to AA.

The AA will perform the basic or extended path validation process to verify that credentials have not been revoked. The provided certificate could also consist of a short-term certificate based on an underlying pseudonym solution. On successful validation, the AA will then issue to the vehicle the corresponding ABCs. ABCs will include encoded certificate's information, such as, the expiration date, the $Cert_{ID}$, revocation information, etc. Additional information needed to generate presentation tokens will also be included.

5.1.2.3 Presentation Tokens

Tokens are data artifacts that contain the required information, and the support cryptographic evidence, which are exchanged between the vehicles and the service providers. A token is generated from the vehicle's /driver's P-ABCs, and in ABP are assumed to be pseudonym-based and therefore unlinkable (a SP cannot tell if two different tokens were derived from the same credentials), unless the token has been intentionally generated to reveal linkable information (e.g. in case of liability) the AA could trace back the underlying credentials. In general, a token will be generated specifically to meet the corresponding SP's conditions in order to grant service access. As a result, when a token has been generated, it will be attached to the vehicle's request. On reception, the SP will perform two different actions, *i)* the token-certificate related validation through the AS, and, if positive, *ii)* the ABC validation of the token.

5.1.2.4 Credentials Revocation

In ABP, the revocation of credentials will be done by the AS, providing near-real time certificate validation via the multi-CA OCSP component. In addition, since certificates issued by the AS are short-term, the related P-ABCs will be regularly updated, in particular the non-revocation evidence attribute.

5.1.2.5 Providing Minimal Information Disclosure

This section presents the communication flow of the ABP, and how the minimal information disclosure could be achieved in an inter-regional scenario, next credential issuance will be described.

1. A vehicle, $vehicle_1$ with a certificate issued by the CA_1, travels to a different domain infrastructure.

2. Once crossing the inter-regional border, $vehicle_1$ requests a set of P-ABCs to the current infrastructure, by providing its certificate issued by the CA_1.

3. The infrastructure which belongs to a domain with a CA, CA_2, since CA_1 is unknown, the infrastructure performs the extended path validation introduced in Section 4.2.3.

4. If the certificate of $vehicle_1$ is valid, the CA_2 will then issue a set of temporary P-ABCs, so the vehicle will be able to interact with the current infrastructure with no need to perform further validations.

After the credential issuance has been successfully performed, $vehicle_1$ will be able to communicate with other vehicles and services with a local-domain validation. Now imagine a second vehicle, $vehicle_2$, requesting information related to the driver's license of $vehicle_1$. For the $vehicle_1$ to verify is an authorized entity is requesting the information, the following steps must be done.

1. $vehicle_1$ received a message requesting information related to the driver's license.

2. Before granting any access to the information, $vehicle_1$ requests to $vehicle_2$ to provide a token that can prove that $vehicle_2$ is an authorized entity, (e.g. by proving the type of entity or an associated trust level).

3. $vehicle_2$ generates and presents a token proving that is an authorized entity (probably this information is disclosed), and that its associated trust level is equal or greater than the one required to access the information.

4. $vehicle_1$ performs both validations, on the associated certificate (issuing CA, status of certificate, etc), and on the P-ABC that meets the defined conditions.

5. Upon successful credential's validation, $vehicle_1$ selects the attributes from the associated driver's license, generates the token, and presents it to the $vehicle_2$.

6. $vehicle_2$ also performs the two validations on the information received.

Look that, this scenario suits the minimal information disclosure, since, vehicles are able to decided on which attributes should be disclosed, meaning that, the $vehicle_1$ only needed to provide evidence that the associated driver's license was valid and there was no need to disclosed for example the driver's nationality that is currently visible in non-digital driver's license.

5.2 Providing Anonymity and Unlinkability in VANETs

Privacy in vehicular networks can be considered from different perspectives: *i)* identity privacy (linking an identifier to an user or vehicle, *ii)* location privacy, which includes speed, position and traveling routes, and *iii)* data privacy, which includes not only information contained within the vehicle such as license plate and driver's identifiable information, but also by means of services requested by the users/vehicles which leads to user profiling. So far, most of the research efforts done in the privacy of VANETs have focused only in protecting user identification and implicitly user's location giving very little attention to the information contained in vehicular communications. While identity and location privacy have been addressed by proposing a wide range of pseudonimity solutions, pseudonymity cannot prevent an attacker from collecting other user's related data; thus, user profiling can be achieved just by the passive collection of communication information regarding vehicles' activities, just by the simply contents of their queries. The main objective of this section is to cope with the privacy issued the lead to user profiling, by proposing an anonymous information retrieval protocol mainly based on user collaboration to privately retrieve information from Service Providers (SPs)

5.2.1 Introducing Query Forgery and Permutation

The proposed protocol is based on the one presented by (Rebollo-Monedero *et al.*, 2010), which relies on the concept of query forgery. Query forgery refers to the

process of attaching bogus queries (1 or more) to the authentic ones, in order to prevent an attacker or service provider to learn about users real interests, meaning that, if just one user intends to query a service provider, the same user will send two different queries and the service provider will not discern of which matches the user's real interests. In addition, two different approaches were introduced *i)* query permutation on a chain of users and *ii)* query permutation of a trellis of user. In the query permutation process, a number n of collaborating users attach their queries and change the order of them before delivering to the corresponding service provider, the approaches aforementioned differ from the form users are organized to collaborate (chain and trellis) and thus, provide a different privacy degree. Due to the special characteristics that are inherent to a VANET system, this protocol focuses on the query permutation considering a chain of users rather than a trellis of users, since in VANET is of utmost importance to consider the performance issues derived from these type of solutions.

5.2.2 Assumptions

Before describing further details of the proposed protocol in a given scenario we shall first introduce the considered assumptions corresponding to the vehicular communication system and participant vehicles collaboration.

- It is assumed that neither the SP nor other cooperating vehicles can be completely trusted regarding the disclosure of a user's private information.
- Participant vehicles possess a pseudonym-based (short-term ID), managed by an existent solution (e.g. previously proposed ABP for VANETs).
- Relying in the ABP protocol and presentation tokens, SPs are able to verify is the entity requesting a service meets the required conditions.
- Services are provided in a "flat-rate" fashion where accountability is not an issue.
- Vehicles mobility is spatially restricted and spatially dependent due to the mobility patterns already defined by the infrastructure.

- Temporary group navigation is possible due to the geographical proximity and spatial dependency of vehicles.
- Messages exchanged by vehicles and SPs might be encrypted.
- Both queries and replies contain accurate information that may not be perturbed.

5.2.3 Querying The Infrastructure

The proposed privacy protocol specifically aims to provide unlinkability by preventing unauthorized disclosure of vehicle's queries. This approach assumes the existence of a pseudonym generation mechanism/solution that protects users' real identities, being aware that: pseudonyms provide temporary anonymity, but the sole use of pseudonyms cannot prevent the whole user profiling process. Technically, the protocol is independent of the underlying security solution, although the presented scenario relies on the existence of a pseudonym solution achieved thanks to the implementation of attribute-based credentials, which in turn relies on a PKI-OCSP based protocol including a set of traditional cryptographic mechanisms able to prevent the unauthorized disclosure of the messages exchanged by vehicles and SPs. The protocol also advantages VANET's unique features by relying on the existence of a cooperative structure of vehicles, which is possible due to the fact that, vehicles travel along trajectories with geographical proximity to other vehicles and making possible to navigate as a group. In the following the main scenarios are described.

5.2.3.1 Vehicle Query Forgery - Simple Use Case Scenario

In the simple use case scenario, when a single vehicle must request a service from the Service Provider (Figure 5.2), vehicle simply sends the query via RSU. With the given scenario, either the RSU or the SP could relate the information of the query to the actual vehicle. By implementing the query forgery concept, the vehicle generates a forged query and send it along with the authentic one just as illustrated in Figure 5.3, in order to ensure that a SP or any attacker overhearing the communication cannot completely ascertain the vehicle's current information

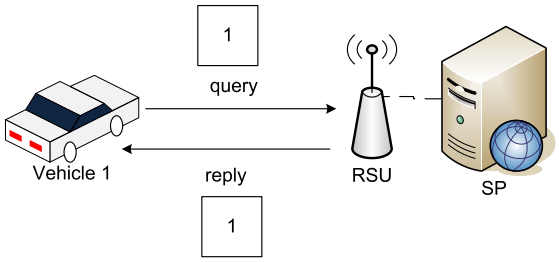

Figure 5.2: A vehicle requesting a service - simple query scenario

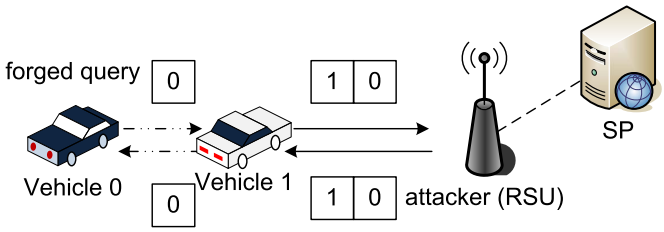

Figure 5.3: A vehicle requesting a service - forged query scenario

interests. As shown in Figure 5.3, the authentic query is labeled with '1', and the forged one, with '0'. Thus, the SP cannot discern which of the submitted queries is authentic or matches user's real interests.

5.2.3.2 Vehicle's Query Permutation - Extended Scenario

In the single-user case of Section 5.2.3.1 the transmission of two queries could be regarded as the collaboration of two different vehicles, each of them submitting a different query to the service provider, as a result, the service provider could not discern which query belonged to whom. Note that a RSU could act as an intermediate in the communication between vehicles and services providers, but could also be referred as a service provider itself. In the following an extension of the scenario described in (Figure5.3), which is based on vehicles' collaboration will be introduced. Based on the concept of query permutation on a chain of users introduced in Section 5.2.1. This scenario consists of n vehicles which form a chain. In this scenario the first vehicles, represented by *vehicle 1*, attaches two different queries, an authentic and a forged one in random order, and forwards

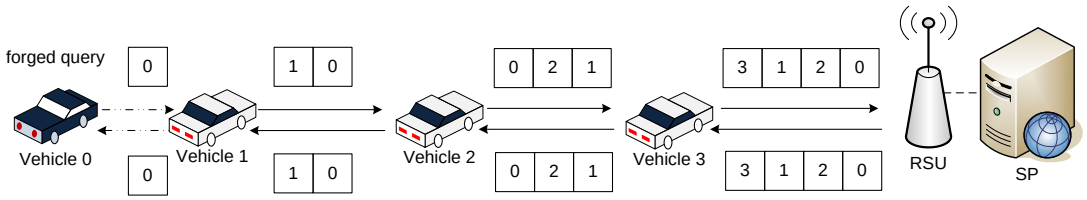

Figure 5.4: Service request through vehicles collaboration - forged query permutation scenario

them to a second vehicle represented by *vehicle 2*, willing to participate, that is, a vehicle with a clear intention of requesting a service. In turn, *vehicle 2* generates its own query, and then produces a random permutation of the queries, labeled in Figure 5.4 as '0','1' and '2', respectively. The randomly permuted list of queries is therefore sent to a third vehicle, *vehicle 3*, which performs the same steps as *vehicle 2*. Theoretically, a maximum number of n vehicles could collaborate, where, the last vehicle, *vehicle n*, will deliver to the service provider a random permutation of *(n+1)* queries. In this scenario, neither the provider nor the intermediate vehicles or RSU could know for certain which authentic query was generated by which of the vehicles.

To deliver the corresponding $(n+1)$ replies generated by the SP, the process is reversed as shown in Figure 5.4.

5.2.4 Anonymous Information Retrieval (AIR) Protocol

The proposed approach could be implemented in two different operation modes namely single query and group query communication, which somehow follow the scenarios described in Sections 5.2.3.1 and 5.2.3.2 respectively.

5.2.4.1 Single Query Communication

This operation mode is the simplest and basically relies on the assumption that there is no need for a previous establishment of a communication group to achieve certain degree of privacy. Similar to Section 5.2.3.1, in this scenario, the first vehicle, *vehicle 1*, transmits two queries (authentic and forged) as the collaboration

of two different vehicles (real and imaginary). On reception, intermediate vehicles $(n-1)$ might be willing to participate, and taking advantage of the already started process, insert their own queries and perform the query permutation process, so that, a better degree of privacy could be achieved. Note that in the worst-case scenario, the SP will received only two queries. To deliver the corresponding replies, a similar process must be performed, *vehicle n* will delete its own query from the list and reverse the permutation before sending it to vehicle (n-1). A important advantage is that because no previous group communication must be established a better performance degree could be achieved. On the contrary, the main drawback of this approach is that provides a higher vulnerability to statistical privacy attacks.

5.2.4.2 Group Query Communication

Opposite to the single query communication,in the group operation mode, the initiator vehicle must first establish the group by performing the following steps:

1. *Vehicle 1*, initiates the handshaking process, by sending a "join group" request to its neighbors[1].

2. Once a number of acknowledgments are received, *vehicle 1* will automatically evaluate a set of parameters such as speed, direction and distance to be able to select potential participants. At the application level this can be achieve by implementing approaches such as the one described in (Borsetti *et al.*, 2009)

3. On selection, queries will be inserted and forwarded by the members of the group following an order determined by a hash function, in order to prevent strategic ordering of vehicles and therefore avoiding collusion attacks.

A clear advantage of the group operation mode lies in the fact that with collaborative participation a higher privacy degree could be achieved. However, the main disadvantage consists in the group establishment, not only from the performance perspective, but from the dynamic nature of a VANET, nodes might leave the communication range once agreed to participate.

[1]Nodes within communication range, typically within 250m distance

Type	Information
JoinGroupReq (R')	$R' = \{ID \| \| location \| \| timestamp \| \| payload\}$
AckGroupReq (A')	$A' = \{ID \| \| location \| \| timestamp \| \| payload\}$
Query	$Q_n = \{Query \| \| Q_{ID}\}$
Single query message (M)	$M = \{Q_n \| \| ID_n\}$
First vehicle message (M')	$M' = \{Q_n \| \| Q_{n-1} \| \| ID_{n-1} \| \| ID_n\}$
Multiple query representation (M'')	$M'' = \{Q_n \| \| Q_1 \| \| Q_{n-1} \; ..ID_{n-1} \; \| \| ID_1 \; \| \| ID_n \; \}$

Table 5.1: Messages and queries definition

5.2.4.3 Message Definition

In vehicular communications, participant nodes exchange different types of messages, Table 5.1 shows the minimum information required by each of the messages that are exchanged in the proposed protocol. In Table 5.1 the ID parameter refers to a PseudoID (based on anonymous credentials) and the payload may contain additional information such as vehicle direction and speed. The minimum number of exchanged messages for the different operation modes is then determined as follows: For the single query communication mode, the total number of exchanged messages will be 2 ($M' + (n-1)M''$). In the group communication operation mode, the initiator (first vehicle) will additionally broadcast a message R' and process a number of $m(A')$ messages. To provide confidentiality to queries, each vehicle will encrypt its query with the SP's public key SP_{pk}. This on one hand will protect the queries in such a way that collusion attacks would imply SP's participation. In addition, replies might also be ciphered with a temporary key (session key) V_{tk} included in the message, and that cannot be linked to the user's real identity, and will prevent the unauthorized disclosure of the reply.

5.2.5 Discussion

The Anonymous Information Retrieval protocol is aimed at providing privacy and unlinkability regarding both queries and replies for all collaborating vehicles to reduce user profiling. Under the general assumption that neither vehicles nor RSUs or SPs could be completely trusted. That is, if an attacker by any reason, determines the link between two or more different pseudonyms might be able to

automatically evaluate a vehicle's position and/or trajectory, but will not be able to disclosed vehicle's requested services or particular interests. Even in the case, where a pseudonym could be linked to driver's real identity, a complete profile of the driver and his activities could not be automatically generated. Note that, in principle, for each $1 < v < n$, vehicle's v privacy can be completely compromised only if the two participant vehicles in positions $(v-1)$ and $(v+1)$ in addition to the service provider, collude to compare the information available to them (list of queries and replies). Nonetheless, for this approach to be achievable, still open issues must be taken into account. In particular efficiency in vehicular networks has become a major concern; the dynamic nature of VANETs' v2v and v2i communications required a real-time transmission of information. In order to fulfill the given real-time requirements, the privacy solution must be effective and provide an acceptable performance in terms of computational and bandwidth needs. Since, in the presented mechanism the number of queries and replies will remain as $(n+1)$, which obviously imply more computational and bandwidth overhead. In a similar form, the size of the packet will increase according to the number of participants, specially when considering the cryptographic information that will be included to provide confidentiality. Thus, the maximum number of participating vehicles should also be taken into consideration. It is worth to mention that, current approaches aimed a preventing user profiling in v2i communications, have only considered the use of pseudonyms, which, as explain in this chapter is not enough. Different authors have proposed the use of vehicular groups along with a group signature scheme (Section 3.4), to provide anonymous access to location based service applications in VANET. A clear disadvantage is the general assumption that the group leader can be completely trusted.

Chapter 6

Context-based Trust Validation

In privacy-conscious environments (e.g. eHealth), it is a common belief that individuals should be able to keep and manage access to their personal information, for example by choosing to which entities their personal data should be disclosed. This chapter focuses on VANET's data privacy and trust management from the driver's centric approach, which is founded in a Context-Based Trust Validation Model (TVM) introduced next.

6.1 Introduction

Inspired by eHealth systems, which highly demand the protection of a patient's personal data. The Trust Validation Model (TVM) focuses on the trust evaluation of entities for protecting driver's personal information from being disclosed to unauthorized parties and, at the same time, to enable decision making based on the trust level assigned to the communicating entities. In other words, the driver's explicit consent authorizes two different tasks *i)* disclosing his personal identifiable information, possibly stored in the vehicle (e.g. electronic license plate, driver's license, etc.), or by presenting certain attributes that could be categorized as private information, and *ii)* processing received information(e.g. safety message) on intermittent infrastructure-less scenarios, where an online validation with the infrastructure, cannot be always performed, a further description of these two scenarios is presented next, which will allow the definition of the necessary components of the TVM introduced in Section 6.3.

6.2 Use Case Scenarios

This section defines two infrastructure-less scenarios, where due to the lack of v2i validations (Section 2.1.1), a security vulnerability exist and must be mitigated by implementing additional mechanisms.

Scenario 1: Private Information Access Vehicles are considered highly personal devices that are kept for long, and as discussed in Chapter 2, will be able to store great amounts of information, including private information, therefore unauthorized access to such information should also be carefully considered. Let's take for example the scenario where a vehicle, $vehicle_1$, is requesting private information of the driver/vehicle (e.g. past locations) of $vehicle_2$, assuming that, the requesting entity, $vehicle_1$, is an "emergency vehicle" just as shown in Figure 6.1. This 'basic' scenario, raises a few questions: *i)* if messages in VANET will be sent anonymously, how does the $vehicle_2$ verifies the type of entity of $vehicle_1$, *ii)* how can the trust level of $vehicle_1$ could be defined and therefore validated?,*iii)* under which circumstances will $vehicle_2$ disclose the information, and moreover *iv)* which information should be disclosed?.

To be able to answer this questions, it is important to define the context in which the access to the information will be granted, and exactly what type of information will be accessed. The context of the information will then support the trust validation process that will ultimately allow vehicles to take the appropriate decisions.

Scenario 2: Messages Processing Broadcasting messages to warn drivers about different situations, is one of the most important applications in VANETs. Imagine that, a vehicle, $vehicle_1$ receives a number n of "warning" messages from supposedly n vehicles reporting an accident a few kilometers away, just as depicted in Figure 6.2. This scenario, which is expected to become a common scenario in VANET's safety applications, and where messages are sent anonymously, raises a very important question: how will $vehicle_1$ know if messages should be trusted?.

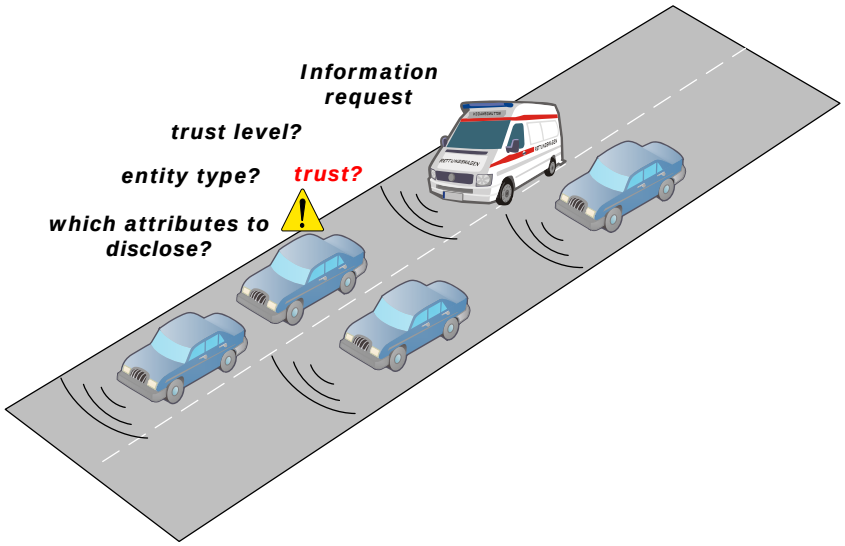

Figure 6.1: An emergency vehicle is requesting private information to another vehicle on the road.

To be able to answer that particular question, it is of utmost importance to learn about the current situation or context, e.g. how many messages were received?, were all messages originated from the same vehicle?, what kind of entities were involved?, from which direction are messages coming? and how fresh are these messages?. To cope with these issues, it is necessary to provide a component able to validate the trust level by evaluating the context parameters that will be provided, and therefore reject or accept the message by for example lowing the speed, taking a different route, etc.

As it can be observed, in both scenarios it is necessary to implement a mechanism able to evaluate the overall trust level defined by the combination of different variables provided by the context. Based on the trust level, vehicles then will be able to take the appropriate decisions.

6.3 Trust Validation Model

The Trust Validation Model (TVM) mainly supports decision making, by evaluating the trust level of contexts derived from the aforementioned scenarios. The

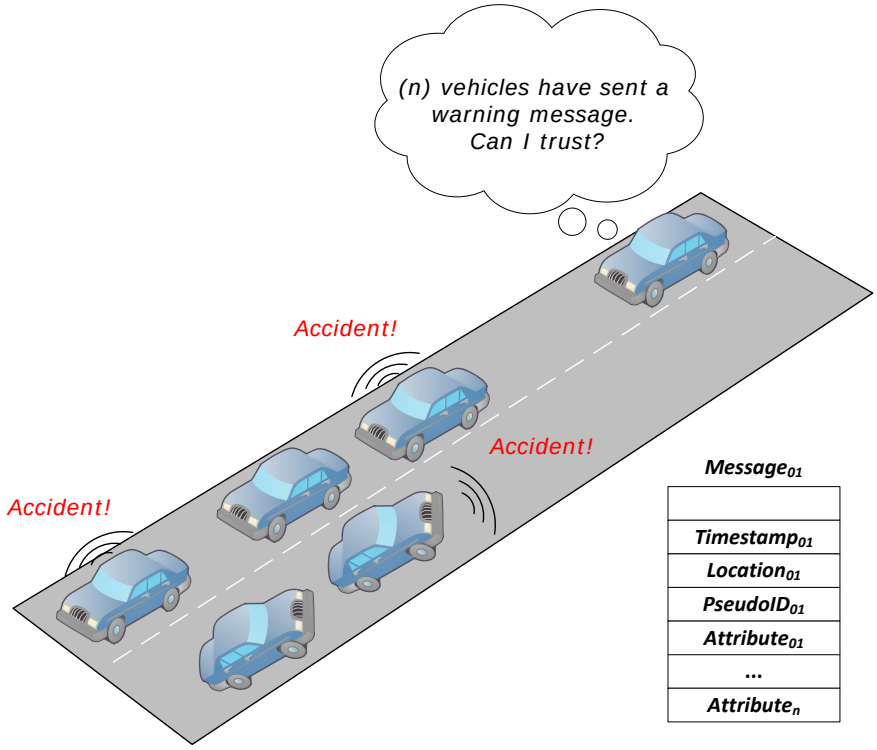

Figure 6.2: A vehicle received n warning messages reporting a road accident.

TVM, first classifies the type information contained in the vehicle and the type of messages to be exchanged by assigning different labels to the information according to its sensitivity level, secondly, validates the sender's or requestor trust level, according to a set of attributes previously assigned, and mainly based on the role and the type of an entity along with other context information. This process is achieved thanks to the proposed P-ABC protocol presented in Section 5.1.1. Finally, it matches the context information with a pre-defined policy, which, in turn will specify the action that should be performed.

Before further describing the TVM, it is important to mention that, the TVM relies in the following assumptions:

- The existence of Tamper Proof Device (TPD) or Trusted Platform Module (TPM) able to store security information and perform crytographic/secure operations.
- The communications in the covered scenarios, are done anonymously.
- Trust validation can be performed even if no "online" validations via *v2i* communications are available.
- As already mentioned, the existence of an attribute-based solution is assumed, in this proposal the TVM takes advantage of the P-ABC protocol.

Next, the basic concepts behind the information classification will be clarified.

6.3.1 Information Classification

For the sake of simplicity initial classification of the information will be performed in correspondence to the type of scenarios aforementioned. However, any driver should be able to establish its own classification according to his particular privacy and trust concerns.

6.3.1.1 Private Information

Private information refers to all kinds of information that could be stored in the vehicle, this obviously, includes attribute credentials and the attributes to be

disclosed to corresponding authorized parties. In this classification, Information Labels (IL) will be assigned according to the corresponding scenario, and, the required privacy level (from now on referred as the Global Security Level (GSL)[1]) to access it will be assigned, note that, the privacy level assigned to the information, should correspond to the *GSL* provided in the TVM (further discussed in Section 6.3.3. An example of labels that could be applied are described next:

- Liability: private information that should be disclosed to authorized parties only in situations where liability is required (i.e. authorized law enforcement agents);
- Emergency: information that should be disclosed to authorized parties in emergency situations (i.e. emergency vehicle -paramedics).
- Services: information that should be disclosed to services offered by the infrastructure (e.g. when accessing infotainment applications). Note, that this information is application related, and will strictly depend on the services available in the infrastructure.
- Personal: information that should be disclosed to authorized parties for example to interact with known vehicles when traveling in groups.
- Public: information accessible to any party, no privacy checks are required by the own vehicle in order to be disseminated. In turn, receivers might need to perform trust validations, in order to decide whether or not received information must be trusted, which is strongly related to the classification presented next.

6.3.1.2 Public Information

This classification refers to all the information in VANETs that is public to its participants, and that it is no precisely stored in the vehicle, but in turn is represented by commonly exchanged messages with the main objective of informing

[1]Terminology defined by the REM methodology Section 4.2.3.2

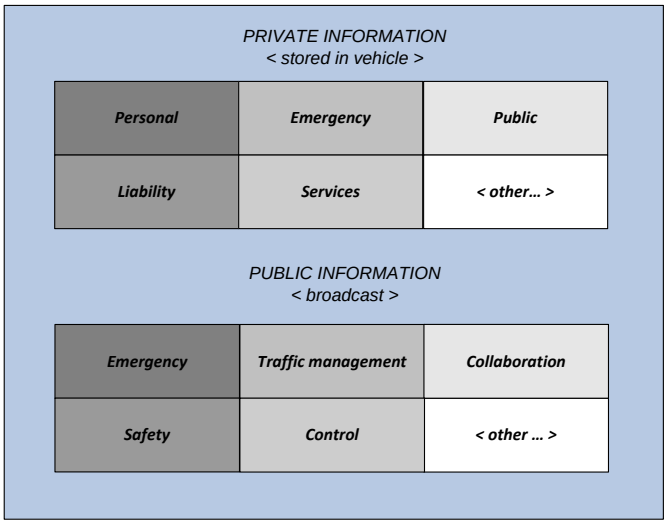

Figure 6.3: Generic Classification of Information.

vehicles about various situations, such as, traffic management, emergency warnings, or nodes misbehavior. Therefore, within this classification, information could be labeled as follows:

- Emergency: public information about emergency situations such a fatal road accidents where actions are required and therefore must not be ignored.
- Safety: public information mainly about road conditions, specially aimed at preventing potential accidents.
- Traffic management: public information to alert vehicles about traffic congestion, aimed at improving the traffic flow, where actions such as lowing the speed, or changing trajectories might be required.
- Control: public information that is periodically sent in the form of 'hello beacons'.
- Collaboration: information that will be disseminated to request vehicle's collaboration such as group forming to various objectives.

As it can be inferred from Figure 6.3, classification of messages could also be extended, naturally considering the driver's trust concerns, since in most of them,

different actions are required, additionally a trust level referred also GSL should be assigned. Nevertheless, before trust-based decisions can be taken either for an entity willing to access driver's private information or to decide whether or not to trust any received public information, its is mandatory to perform a trust evaluation on involved entities' attribute credentials, next section introduces the relation between VANETs involved entities and their corresponding trust levels.

6.3.2 Defining Entity's Trust Level

Trust Levels (TLs) will be provided to entities participating in VANETs in the form of attribute to be disclosed in different scenarios such as the ones described in Section 6.2. In order to define what level of trust must be assigned to vehicles, first, a general classification of vehicles must be done, the type of the vehicle will be referred as Entity Type (ET). Note, that vehicles can be classified according to a wide range of parameters. However, in the proposed context only the vehicle's 'role' will be considered. As a result, a ET can be for example emergency, police, traffic authority, private vehicle, etc. Initially, a default TL could be assigned by authorities issuing credentials and the TL will correspond to the ET of the vehicle.

- Zero Trust: $(TL = 0)$, an entity which trust level cannot be validated or that, actually posses a zero trust value (further discussed in this section).
- Low Trust: $(TL = 1)$, first level of trust that can be assigned by default to private vehicles.
- Medium Trust: $(TL = 2)$, second level trust that can be assigned by default to regional authorities such as police vehicles or traffic authorities.
- Semi-full Trust: $(TL = 3)$, third level trust, that can be assigned bye default to emergency vehicles, and other related authorities.
- Full Trust: $(TL = 4)$, fourth level trust assigned either to enforcing law authorities in liability cases, or manually assigned by the driver to an entity which is well known and fully trusted.

Note that with the implementation of reputation systems or any other solution, able to detect both misbehaving nodes and collaborating ones, it is very likely that the default assigned values will change. In this scenario, credentials, will be updated to the new TL level, where, misbehaving vehicles could loss credibility when decreasing their default TL or become some kind of reference when, due to collaborating behavior the TL is increased. Therefore a TL namely 'Untrusted' with a ($TL = -1$) is also defined, specially for misbehaving vehicles during the warning period[1]. In summary, the combination of the TL and the ET attributes, will partly define the context in which information could be trusted or disclosed. Next section introduces the TVM main components, followed by the description of the main processes.

6.3.3 Model Components

- Credential Validator: Provides the necessary mechanisms to validate the provided P-ABCs.
- Information Classifier (IC): This module determines the type of information, that has been requested or has been received. Once the information type has been identified, obtains the corresponding GSL required to perform any action defined in the corresponding policy.
- Context Manager (CM): This module is in charge of storing for time *(t)* (a pre-defined time interval), context information, that will be provided to the TE enabling the GSL validation.
- Trust Evaluator (TE): This module establishes different context scenarios in order to validate the corresponding GSL needed to match any pre-defined policy.
- Policy Manager (PM): This module provides the mechanisms to be able to define, validate and match any pre-defined policy. Based on the information received from the rest of the modules, matches the corresponding policy, and, upon results an action can be performed.

[1] Assuming that, vehicles will not always operate in the same mode.

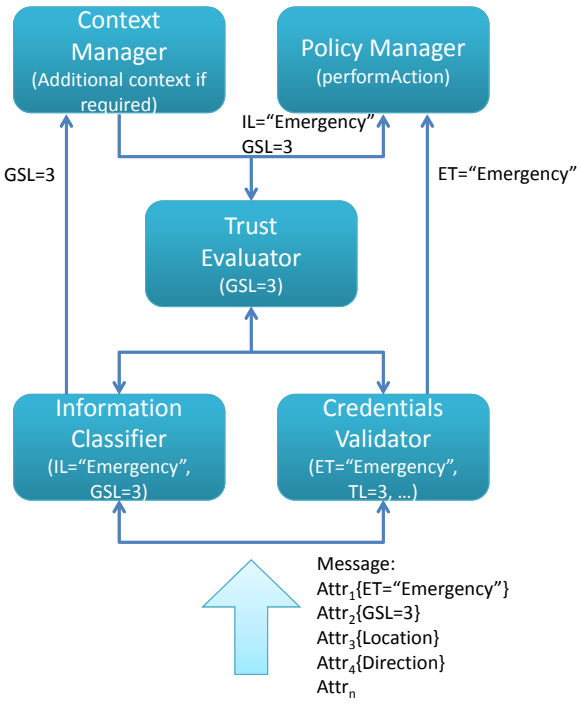

Figure 6.4: Communication flow among the TVM components.

6.4 Trust Evaluation Communication Flow

Going back to the scenarios described in Section 6.2, this section will illustrate how will trust validation will be achieved, by describing the main flow among the different components of the TVM, just as shown in Figure 6.4 . Access control will be introduced next, followed by the message processing scenario.

6.4.1 Context-based Access Control for Private Information

A VANET's vehicle is able to request any available service to the infrastructure, but at the same time can offer and request "services" to other vehicle. Let's take for example the scenario depicted in Figure 6.1, an emergency vehicle requesting information. The vehicle will need to identify first which entity is requesting information, to be able to select the corresponding attributes that might be dis-

closed. However, since the communications are assumed to be done in an anonymous fashion, how will the vehicle perform the authorization checks and decided whether or not the access to its information will be granted?. To achieve this goal, on one hand the driver/vehicle can decide which personal information can be accessible and the minimum required security level to access such information, and on the other hand the requestor should provide the necessary attributes that will allow the vehicle to perform the trust validation.

In Previous research (Serna *et al.*, 2008) a Mandatory Access Control (MAC) model was proposed. The MAC model performed the evaluation of a TL contained in the Attribute Certificate (AC) of the requestor, and matched the TL with the authorization levels assigned to an entity's personal information. Basically, by relying on *i)* the Simple Security Property (no read-up) and *ii)* the *-Property (no write-down). However, further research identify more complex scenarios where the simple evaluation of an static authorization level was not be enough, therefore, to perform the trust validation of an entity, additional attributes need to be disclosed, which, will be validated by the CV, just as described next.

Credentials validation : $vehicle_1$ receives an information request from $vehicle_2$, for this particular scenario, the CV component performs the validation of two different attributes (i.e. ET and TL), if no credential validation can be performed default values ($ET = Unknown$, $TL = -1$) will be passed to the TE. In this example, it is assumed that the CV could successfully validate the credentials and obtain the values $ET = Emergency$ and $TL = 3$.

Information Classifier : the IC component will then identify the type of information that is being requested in correspondence to the defined labels, lets assumed that for the emergency situation, the information has been labeled as IL="Emergency". Next the IC will obtain the GSL level required for "Emergency" label, let us say $GSL = 3$.

Context Manager : The CM can provide to the TE and the PM additional context information when applicable.

Trust Evaluator : The TE component will receive information from the CV and the CM (if needed), and will then perform context validations and finally assign a GSL level, in this scenario the TL will be directly assigned,(i.e. $GSL = 3$)

Policy Manager : Finally the PM will receive the information from the CV $\{ET = Emergency\}$, the TE $\{GSL = 3\}$, the IC $\{GSL = 3, IL = Emergency\}$,and optionally (scenario-dependent) from the CM, and , through the policy matcher the final validation will be performed, and the action pre-defined in the policy will be executed (i.e. grant or deny access), within the policy matcher, the validation of the GSL will be performed based on the properties defined in the described MAC model.

Note, that if any other authoritative vehicle possess the same TL, because the TE will be different, will not be able to retrieve information with $IL = Emergency$ if not explicitly defined in the policy, which with the previous model (MAC)could not be achieved. Moreover, as mentioned before, because of the behavior of vehicles, the TL might change in time, thus for a misbehaving emergency vehicle, let us say with $TL = 1$, even though the ET will prove that is an authority, because of its TL the information access will not be granted. Next a more complex scenario will be discussed.

6.4.2 Context-based Information Trust

This section defines the communication flow among components of the TVM, in scenarios where public information is disseminated in order to alert other vehicles of an event, and for a vehicle to be able to execute any action a trust validation must be performed. In particular, this section takes as reference the scenario presented in Figure 6.2, where a vehicle, $vehicle_1$ receives n number of warning messages, from supposedly n vehicles reporting a road accident. In the next sections two important processes namely *i)* context validation definition and *ii)* policy definition are described, followed by the communication flow definition.

6.4.2.1 Defining the Context Validation

The TE component is in charge of performing trust validations with an output represented by the GSL. Trust validations might depend on the context information, thus, different validations could be performed from one scenario to another. This is mainly because trust validations are mostly user-defined, and strongly dependent on the driver's privacy or trust concerns. In other words, similar to policy definition, the user defines which context information must be considered for each of the defined scenarios, and based on those specifications, a set of attributes (e.g. location, pseudoID, ET, TL, etc.) will be validated, to match either all possible scenarios or only specific ones. Focusing on the aforementioned scenario, where $vehicle_1$ receives warning messages to alert of an accident, deciding whether or not to trust, could be supported if a number of conditions are met. This conditions are established in terms of context information, to be more specific, if $n = 1$, meaning that $vehicle_1$ receives only one warning message, from a vehicle which credentials could not be verified i.e. ($ET = Unknown$ and $TL = -1$), it can be obvious that the message will be discarded. However, if in the context validation definition, a minimum threshold $min_M = m$ has been defined, and $n \geqslant min_M$, trust validations will provide a different outcome. Now imagine a more complex scenario, where more than one condition should be met, e.g. a minimum threshold of messages $min_M = m$ belonging to entities with a $TL \geqslant min_{TL}$ if all conditions are met, probably the GSL will be calculated as in Equation 6.1, however, if conditions are not met, the lowest TL value could be directly assigned i.e. $GSL = TL$. As it can be inferred, the definition of the context validation can be customized according to each driver's concerns. In a similar form, policies will be defined, just as presented next.

$$GSL = int(\frac{\sum_{i=1}^{n} TL_i}{n}) \tag{6.1}$$

6.4.2.2 Evaluating Information Trust

Going back the scenario 2 presented in Section 6.2, and assuming that in the TVM, the TE has already a context validation defined and policies have been

established, the TVM will implement the following validations.

Credentials validation : $vehicle_1$ receives a number n of "warning" messages from supposedly n vehicles reporting an accident a few kilometers away, for this scenario, the CV component performs the validation of three different attributes (i.e. ET, TL and location), if no credential validation can be performed default values for each messages/entity will be ($ET = Unknown$, $TL = -1$), this values are deliver to the TE.

Information Classifier : the IC component will then identify the type of information that is being requested in correspondence to the defined labels, lets assumed that for the warning alerts, the information has been labeled as $IL = Emergency$. Next the IC will obtain the GSL level required for "Emergency" label of public information, let us say $GSL = 4$.

Context Manager : The CM will provide to the TE and the PM additional context information when applicable, for this scenario,the PM will provide additional information regarding vehicles locations, ETs, and possibly direction or speed, the TE will evaluate the context information such as if the n come from different 'locations'. This is done because it is not easy to discern if the n messages come from a single $vehicle_n$ using n pseudonyms or they actually come from n different vehicles, thus additional attributes should be validated, considering that first alerts do not reach any of the defined threshold and the $GSL = 1$.

Trust Evaluator : The TE component will receive information from the CV and the CM, and will then perform context validations and finally assign a GSL level, in this scenario the TL will not be directly assigned, since different threshold have to be met to get one value or another for the GSL.

Policy Manager : Finally the PM will receive the information from the CV $\{ET = Emergency\}$, the TE $\{GSL = 1\}$, the IC $\{GSL = 4, IL = Emergency\}$, and optionally (scenario-dependent) from the CM $\{location_1, \ldots, location_n, attr_1, \ldots attr_n\}$, and , through the policy matcher the final validation will be performed, and the action pre-defined in the policy will be executed (e.g. discard, reroute, etc).

Chapter 7

Analyzing the trade-offs between security and performance

The unique characteristics of a VANET highlighted in Chapter 2, require the adoption of security protocols with little impact on the overall system performance, but at the same time secure enough to achieve the drivers' trust. This chapter shows empirical results obtained from our quantitative analysis and simulations, and discusses them from both performance and security perspectives.

7.1 Introduction

In previous chapters, different security and privacy protocols that mainly work at the application layer have been introduced. However to assure their feasibility and integration within a mobile network, a set of specific VANET constraints must be taken into consideration. In this chapter it will be quantitatively demonstrated that the proposed protocols do respect these constraints. At this aim, a set of experiments has been designed, mainly consisting of an hybrid approach that includes *i)* the evaluation of the implementation of main cryptographic protocols discussed in Section 4.6 and, *ii)* their simulation to evaluate the incurred transmission delays generated by the messages' security overhead (Section 7.2.1). We analyze the proposed protocols' performance in terms of the communication time required for each one of the exchanged messages. The overall communication time (Raya & pierre Hubaux, 2005) (Xiaodong *et al.*, 2008) is represented as

Message ID	Format	Type
M'	$\{location\|\|timestamp\|\|message\|\|pseudoID\}$	*Without Security*
S'	$M' + Sig_{Sk}\ \{M'\}$	*Signed Message*
A'	$M'\ \|\|Cert_{ID} + Sig_{Sk}\ \{M'\ \|\|Cert_{ID}\}$	*Authentication Message*

Table 7.1: Signed and authentication messages format

the sum of all the processing and transmission delays from the messages in any of the proposed protocols for both v2v and v2i communication. In this proposal, the evaluated times take into consideration two factors:

1. The total communication time for a single message in both v2v and v2i scenarios.

2. The number of exchanged messages by each one of the proposed protocols.

7.2 Communication Time Estimation

It is expected that vehicles in a VANET will generate signed messages with their own private key (*Sk*), attaching the corresponding public key certificate identifier (*CertID*) in order for the relying party to perform the validation processes described in Section 4.6.1. As mentioned in Section 4.6.1, the rationale behind using a certificate identifier instead of the full certificate is basically to keep the security overhead low in the proposed protocols (this will be experimentally demonstrated in Section 7.2.2).

Table 7.1 shows the different types of messages to be exchanged within the security protocols proposed in Chapter 4 and analyzed in this section:

As shown in Table 7.1, authentication messages will only include the CertID, The receiver in turn will extract the corresponding information, verify the signature and validate the certificate. As a consequence, the communication time and also the message size will greatly depend on the cryptographic protocols that are chosen. Thus, the relationship between the security protocols, processes and the

overall communication time (T_p) can be represented as the sum of the 4 main parameters shown in Equation 7.1.

1. Time to format and sign a single message (T_s)
2. Time to transmit the message (T_t)
3. Time to cryptographically verify the message's signature (T_v)
4. Validation time (T_a) -basic or extended path validation on the message -

$$T_p = a \cdot (T_s + T_v + T_t + T_a) \tag{7.1}$$

Note that, signing, verification and validation times (T_s, T_v and T_a) can be directly evaluated, as they depend on hardware nodes and not on the mobility features. On the other hand, the transmission time T_t is affected by vehicle's mobility, speed, transmission rates and packet size. Therefore the T_t will be estimated via simulations.

7.2.1 Cryptographic Overhead

In order to provide greater insight into the performance trade-offs in asymmetric cryptographic protocols, performed experiments will consist of:

1. measuring a message's signature generation and verification times
2. performing a VANET certificate validation process, using the basic and extended path mechanisms
3. performing a set of simulations to determine the transmission delays introduced by the security overhead.

Next, the most representative outcomes obtained for 1 and 2 will be presented, while 3 will be introduced in Section 7.2.2.

7.2.1.1 Signature and Verification Times

At the state of the art, different proposals for implementing PKI in VANETs, have used the Elliptic Curve Digital Signature Algorithm ECDSA- (Petit, 2009) (Blake-Wilson *et al.*, 2002) instead of the RSA cryptosystem (RSA, 2002) typically found in "traditional" PKIs. On the one hand, the WAVE standard specification (Committee, 2007) supports the implementation of the ECDSA cryptographic algorithm for authentication in VANETs, assuming that contrary to RSA, the ECDSA cryptosystem minimally impacts performance. However, this is mainly due to the large size of RSA certificates, which, on the other hand has been extensively adopted by OCSP-based approaches implemented by (e.g. financial institutions). Although recent updates on the RFC 2560 (Santesson & Hallam-Baker, 2010), have introduced support to other cryptographic algorithms such as ECDSA. In order to show the performance trade-offs among the two widely used asymmetric cryptographic algorithms in the proposed protocol, the first experiment consisted of measuring the message generation and verification times, using both the RSA and the ECDSA cryptographic algorithms. Note that the performance of cryptographic algorithms can be strongly affected by the hardware capabilities and the library used to perform them. Over the past few years, different researchers have attempted to demonstrate the performance impact of the two well-known cryptographic algorithms RSA and ECDSA (Petit, 2009), (Martínez-Silva *et al.*, 2007), concluding that ECDSA outperforms RSA, thus making it more suitable for resource constraint scenarios. Taking into consideration that currently there is no agreement about VANETs' on-board hardware capabilities, illustrative measures taken from an experiment done with a Core II Duo 2Ghz processor and 2GB RAM will be presented. All messages, signatures and certificates were generated and verified with the OpenSSL 0.9.8o library (OpenSSL, 2010) using RSA with a key length of 1024bits and an ECDSA with a key length of 192bits. In both cases, the SHA-1 hash function was used. Finally, the percentage of the security overhead is represented assuming that typically, in a VANET, the exchanged messages will be of around 200 bytes (NHTS, 2006).

From Table 7.2 it can observe that, for the obtained times (T_s and T_v) there is not a considerable difference between both algorithms (in fact it was approx-

eSigning algorithm	Signature generation (hash + crypt) time T_s	Signature verification time T_v	Signature size	% security overhead
RSA	*0.009s*	*0.007 s*	*128 bytes*	64%
ECDSA	*0.011s*	*0.011s*	*55 bytes*	27.5%

Table 7.2: Signature generation and verification times

imately 37.5%). Now, considering the total number of messages exchanged by the protocols, our belief is that the generation and verification times will not severely impact the overall performance of the VANET. Moreover, even though RSA slightly outperformed ECDSA, this is probably due to the impact of the cryptographic protocols on the size of the signed messages. ECDSA performs better overall because the security overhead introduced represents only 27,5% of a 200 byte message (whereas in RSA, it represented the 64% of it). Thus, the importance of carefully designing the contents of the each message (e.g. the design decision of using certificate's identifiers instead of the full certificate inside the transmitted messages).

7.2.1.2 Authentication Time Estimation

In order to quantify the validation time required to perform either the basic or the extended path validation (as described in Chapter 4), two periods of time have been measured:

- The time required to cryptographically validate a certificate (basic path validation).
- The time required by the OCSP Responder to validate a certificate (as required by the extended path validation) (OCSP, 2011).

Obtained results are shown in Table 7.3

7.2.2 Transmission Overhead

Due to VANETs special features In VANETs, one of the important requirements is that, the security scheme should be efficient in terms of small communication

Path validation	Validation time (T_a)
Basic path validation (RSA)	*0.006s*
Basic path validation (ECDSA)	*0.007s*
Extended path validation (OCSP Responder)	*0.002s*

Table 7.3: Certificate validation execution times

overhead and acceptable processing latency. To be able to determine the transmission delays introduced by the security overhead, the transmission times of a single message generated including the signature of the different cryptographic protocols are measured. To have a more realistic insight of a VANET system, an experimental simulation aimed at evaluating the packet transmission time(T_t) between two VANET's nodes has been configured. Next section defines the simulation scenario followed by the most representative outcomes obtained.

7.2.2.1 Simulation Scenario

The experimental setup was based on an urban scenario similar to the Eixample district of the city of Barcelona. The scenario consisted of 100 vehicles distributed in a $1km^2$ grid map. The map included traffic lanes and lights, and vehicles with variable speeds between 5-55km/hr, including accelerations and decelerations and a maximum pause time of 2s. The simulation time was setup to 1000s and, during this time, the nodes followed different trajectories in a reflective mode (once the destination was reached, vehicles followed a different trajectory). The nodes' mobility pattern was generated using the Manhattan mobility model with the MobiSim (Mousavi *et al.*, 2007) and the SUMO tool (Behrisch *et al.*, 2011). Simulations were performed with the widely adopted Network Simulator tool (NS2, 2012), considering traffic loads[1] of 15, 25, 35, and 45. The transmission range was setup to 250m, with a transmission rate of 4pckts/s and a data rate of 6Mb.

The packet size was configured according to each scenario corresponding to security overhead introduced by the different cryptographic algorithms; that is 55 bytes for an ECDSA signature (using key length of 192 bits), 128 bytes for a RSA

[1]The number of nodes that simultaneously transmitted information.

Simulation area	$1km^2$
Simulation time	1000s
Type of area	Urban
Routing protocol	AODV
Max queue length	50
Bandwidth	6Mb/s
Node density	100 vehicles
Speed range	5-55km
Transmission range	250m
Message size	{38, 55, 128 and 600} bytes
Transmission rate	4pckt/s =0.25 interval

Table 7.4: NS2 configuration parameters

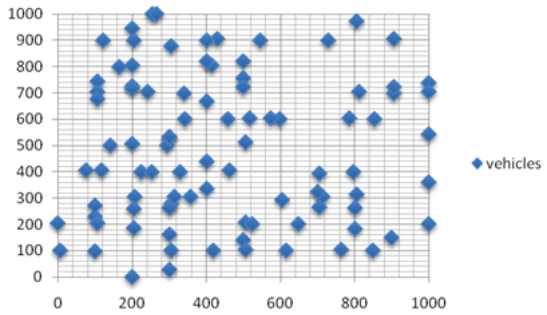

Figure 7.1: Random assigned vehicles spatial distribution

signature (using a key length of 1024 bits), 38 bytes for the ID of the certificate CertID (as defined in Table 4.1) and 600 bytes, considering a X.509v3 standard certificate with ECDSA signature (generated with the OpenSSL library). Table 7.4 summarizes the set of parameters used for the NS2 setup.

The initial distribution of nodes was randomly assigned (Figure 7.1) and the number of connection links was selected according to the different traffic loads. During the simulation time, transmitting nodes where not always in direct communication range with destination nodes (therefore, most packets were delivered via multi-hop).

7.2.2.2 Experimental Results

The results of the incurred transmission delays for both types of signatures are shown in Figure 7.2. It can be observed that with messages of 55 bytes corresponding to the ECDSA Signature, the performance was slightly better than with the 128 bytes of the RSA signature (7ms and 8ms respectively, considering a traffic load of 35 nodes). However, if the overall messages in a VANET are being signed, it is easy to conclude that ECDSA implies a better transmission performance. Moreover, the traffic load is an additional factor that will affect the communications. As shown in Figure 7.2, the transmission delays achieved in a VANET with a traffic load of 40 nodes is almost the double than those achieved while transmitting 25 nodes; therefore, the need to minimize the security information to be included in each packet. Let us, for example, compare the transmission delays of 21 ms corresponding to the 600 byte packets of a full X.509v3 certificate with ECDSA and the transmission delay of 6.8ms incurred by the certificate identifier (CertID), which consists of a 38 bytes packet (according to Table 1), both with a traffic load of 35 nodes. In this case, we emphasize, once again, the importance of carefully designing the contents of each authentication message (e.g. using a CertID in most messages instead of the full certificate inside the transmitted message).

Figure 7.3 shows that if up to 45 vehicles simultaneously transmit information, the packet delivery rate remains above the 95% for a 600 byte message size, which is suitable enough for a VANET environment. However, this can be improved to 98% considering solely the use of a CertID. As for the size of the different signatures, it can concluded that, since the size of the packet remains relatively low there is no significant difference between them and the overall PDR for both is above the 98%. On the other hand, for a traffic load of 45 or more transmitting nodes, we noticed that as the packet size increased, the packet delivery rate decreased. If a congested scenario (more than 50 vehicles transmitting within transmission range) is considered, large packet sizes will drastically impact the number of packets being delivered. Thus, the sole use of identifiers in a message will significantly reduce the packet size (in approximately 93.6% when compared with those messages containing a full X.509v3 certificate attached).

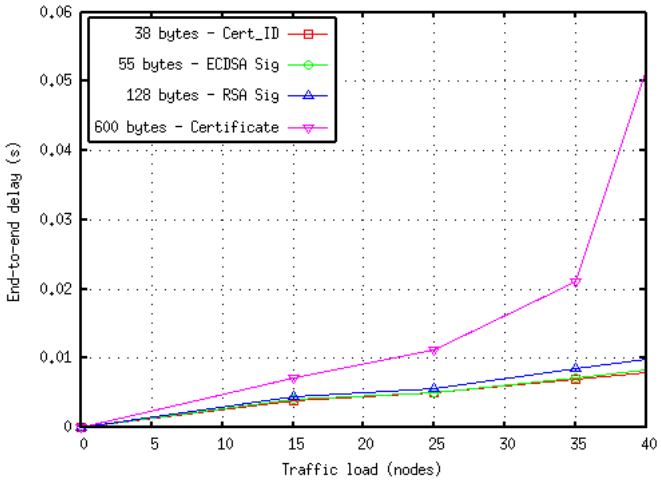

Figure 7.2: Security overhead transmission delay

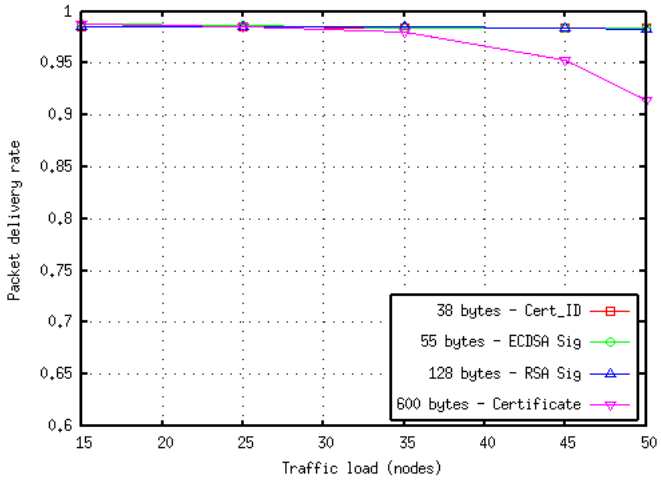

Figure 7.3: Security overhead packet delivery rate

eSigning Algorithm	Message Communication time (s)
RSA	0.030 s
ECDSA	0.036 s

Table 7.5: v2v single message communication time

7.3 Exchanged Messages Computation

As mentioned in previous paragraphs, the overall communication time of the proposed authentication protocol, depends on three factors: *i)* the electronic signature algorithm, *ii)* the security overhead that influences the overall transmission time and, *iii)* the total number of exchanged messages related with the authentication protocol itself. In Section 7.2.1 we have quantitatively evaluated the first two factors (signature, verification and transmission time for a single message); in this subsection will be presented an estimation of the total number of messages needed by the protocols described in Section 4.6, Figure 4.6, Figure 4.5 and Figure 4.7. In particular it will be evaluated the time required by the overall communications introduced by the protocols in terms of messages exchanged and the communication time required for these messages.

7.3.1 Communication Overhead in v2v

For the v2v protocol the minimum number of required messages is: 4. Thus, the overall communication time (T_{cv2v}) can be represented as in Equation 7.2:

$$T_{cv2v} = a \cdot (T_s + T_v + T_t + T_{Alocal}) \tag{7.2}$$

Where, as a derivation from Equation 7.1, T_s represents the time to format and sign a single message and T_v the time to cryptographically verify a messages signature (Section 7.2.1), T_t denotes the transmission time (Section 7.2.2), and T_{Alocal} represents the basic path validation time.In the following table we present the computation of the different timings for a single exchanged message in the protocol:

As shown in Table 7.5 and considering that vehicles will send messages on intervals of 300ms (Armstrong, 2012b), these results prove to be good enough for

eSigning Algorithm	Message Communication time (s)
RSA	0.032 s
ECDSA	0.038 s

Table 7.6: v2i single message communication time

processing received data before creating a new message. As a result, according to Equation 7.2 the overall communication time introduced by the protocol is $T_{cv2v} = 4 \cdot (0.009 + 0.007 + 0.008 + 0.006) = 120ms$ for RSA and $T_{cv2v} = 4 \cdot (0.011 + 0.011 + 0.007 + 0.007) = 144ms$ for ECDSA, note that this values represent the time for authentication in the whole communication process among two vehicles.

7.3.2 Communication Overhead in v2i

The v2i communication protocol requires a minimum of 4 exchanged messages (CertID attached). Again in analogy to Equation 7.1, we represent the overall communication time (T_{cv2i}) as:

$$T_{cv2i} = a \cdot (T_s + T_v + T_t + T_{Av2I}) \tag{7.3}$$

Where: T_s represents the time to format and sign a single message, T_v the time to cryptographically verify a messages signature , T_t denotes the transmission time, and T_{Av2I} represents the extended path validation time. Note, that T_{Av2I} includes the Authentication System time and the OCSP responder time, which according to (EJBCA OCSP) is capable of processing approximately 500 requests per second. The following table presents the timings introduced by the proposed protocol as a result of the experimental results.

In the v2i scenario the extended path validation (Section 4.2.3) is performed, so the computed times increase due to the OCSP responder overhead as shown in Table 7.6. As a result, the total computation of $T_{cv2i} = 4 \cdot (0.009 + 0.007 + 0.008 + 0.008) = 128ms$ for RSA and $T_{cv2i} = 4 \cdot (0.011 + 0.011 + 0.007 + 0.009) = 152ms$ for ECDSA. Notice that in this scenario we have not measured transmission delays within the infrastructure (e.g. communication between the OCSP servers), because from the VANET's perspective the main constrain is the v2v and v2i communication.

7.3.3 Communication Overhead in v2v2i

Finally the v2v communication protocol with infrastructure availability represents a combination of the v2v and v2i scenarios. In this case, the minimum number of required messages is 8, and the overall communication time T_{cv2v2i} becomes:

$$T_{cv2v2i} = a \cdot (T_s + T_v + T_t + T_{Av2I}) \tag{7.4}$$

Where: as in Equation 7.2, T_s represents the time to format and sign a single message, T_v the time to cryptographically verify a messages signature , T_t denotes the transmission time, and T_{Av2I} represents the extended path validation time. In summary, the communication time of a message with either RSA or ECDSA – with extended path validation– will be of 30ms and 37ms respectively. Therefore the total authentication process T_{cv2v2i} according to Equation 7.4 is $T_{cv2v2i} = 8 \cdot (30) = 240ms$ for RSA signatures and $T_{cv2v2i} = 8 \cdot (37) = 296ms$ for EDCSA signatures. These results considered the whole authentication process needed in the communication among two vehicles with infrastructure availability.

7.4 Discussion

Even though PKI-based solutions have been identified as a viable solution (Kargl *et al.*, 2008) (Gerlach *et al.*, 2007) (Parno & Perrig, 2005) (Raya & Hubaux, 2007) and is recommended in emerging standards (Committee, 2007), new approaches which are not based on PKI (Lin *et al.*, 2007), (Mahmoud Al-Qutayri, 2010) argue that the main drawback of the latter is the large size of public key certificates exchanged among vehicles, which significantly affects performance. Typically, the size of a standard X.509v3 RSA full certificate is around 1024 bytes and ECDSA is around 600 bytes, however, as explained in (Martínez-Silva *et al.*, 2007) and (Petit, 2009), by applying different techniques an ECDSA X.509v3 certificate can be reduced. Nevertheless, in our experiments, we have considered 600 bytes as the upper bound of an ECDSA in order to measure the transmission delays incurred from the certificate exchange. In summary, performed simulations have demonstrated that the overall transmission delay of a certificate of 600 bytes is of 10ms, with a traffic load of 25 transmitting nodes, and 20ms, with a traffic load

of 35 nodes, which does not represent a major impact in non-congested scenarios. However, considering that increasing traffic loads will result in increasing delays, to minimize the impact, we propose the use of CertIDs. Looking back to the graph in Figure 4, with a traffic load of 35 nodes, the CertID has a transmission delay that represents less than 50% of the one incurred by the full certificate (9ms and 20ms respectively). Therefore, our design decision of issuing messages with a CertID just as used by the OCSP standard (Myers *et al.*, 1999). Moreover, if we consider two vehicles traveling in opposite directions at the maximum allowed speed (55km/h) in urban regions, the minimal potential communication duration will be of 10s. During those 10s, the vehicles will transmit messages every 300ms, thus the transmission time of a CertID will only represent 3.33% of the 300ms that a vehicle has to spend in order to process a single message. Note that, during the potential communication period, vehicles are assumed to be in each other's direct transmission range (300m). This means that outside the direct transmission range, the potential duration of communication will increase if intermediate nodes are available to deliver messages via multi hop. Note that non-standard certificates such as originally proposed in (NHTS, 2006), could also reduce the total size of the certificate and related communication messages, but as highlighted by the authors, no interoperability will be provided among PKIs. Thus, in EU member states, this solution might not be feasible to implement (take, for example, the electronic National ID cards in the EU, where interoperability was a design criteria from the beginning). Finally, it is also worth mentioning that approaches such as (Borsetti *et al.*, 2009) work at the application level, so that vehicles might be able to select communication nodes according to their geo-location and trajectories (position, direction and speed). This strategy improves the overall protocol's performance by disallowing communication with vehicles traveling in opposite direction and in which the communication duration is considered lower than those sharing similar trajectories

Chapter 8

Conclusions

8.1 Conclusions

This thesis has analyzed general security and privacy issues that are present in VANETs. First, the importance of interoperability for VANET's authentication, along with all the challenges it conveys has been introduced. In order to create secure and dynamic interoperability relationships among untrusted CAs, a security model that makes use an Authentication System (AS) has been proposed. The AS is in charge of performing the contributed Extended Path Validation process by validating credentials in near real-time using the Online Certificate Status Protocol (OCSP) and, quantitatively evaluating a CA's security level through a Trusting CA component that implements the Reference Evaluation Methodology (REM). Secondly, the privacy issues that remained open despite the AS implementation, were extensively discussed. As it has been explained, to be able to provide conditional privacy/anonymity and prevent attacks related to the big brother scenario, additional mechanisms are needed. To provide conditional anonymity and minimal information disclosure, the Attributed-Based Privacy (ABP) protocol has been proposed. The protocol implements Privacy-Attributed-Based Credentials, to selectively select the attributes that should be disclosed to an authorized party. The P-ABCs also implement a pseudonym-based solution able to provide conditional anonymity. Relying on the proposed protocols, a Trust Validation Model(TVM) has been proposed, to address trust validation of entities and support decision making in infrastructure-less scenarios. Finally, an

analysis of the trade-offs between security and performance when implementing inter-vehicular authentication across different PKI domains is presented.

8.2 Future work

Future research directions are aimed at enforcing the TVM in infrastructure-less scenarios, by exploring reputation based systems, and more efficient revocation information distribution mechanisms. As future work, a performance analysis in Privacy-ABC technologies must be done, since in P-ACB technologies there is no commonly agreed framework to identify the pros and the cons. Similar to P-ABCs, in VANETs due to the lack of a real implementations, security approaches are generally evaluated via simulations that are often in very controlled and heterogeneous scenarios, thus the need of establishing a common framework to accurately evaluate and compare different security solutions.

Appendix A

Publications

A.1 Journal

- Jetzabel Serna-Olvera, Valentina Casola, Massimiliano Rak, Jesus Luna, Manel Medina, Nicola Mazzocca. Performance Analysis of an OCSP-Based Authentication Protocol for VANETs. International Journal of Adaptive, Resilient and Autonomic Systems, Vol. 3, No. 1. (2012), pp 19-45

- V. Casola, J. Serna, J. Luna, M. Rak and M. Medina. An Interoperability System for Authentication and Authorization in VANETs. International Journal of Autonomous and Adaptive Communications Systems, Vol. 3, No. 2. (2010), pp. 115-135.

- J. Serna, J. Luna and M. Medina. Geolocation-based Trust for Vanets Privacy. International Journal of Information Assurance and Security, Vol 4 No. 5. (2009), pp. 432-439.

A.2 Conference

- Serna, J., Luna, J., Medina, M.: Geolocation-based Trust for Vanet's Privacy. The Fourth International Conference on Information Assurance and

Security (IAS'08).

- Serna, J., Luna, J., Medina, M.: Trust Management and Privacy for Vehicular Ad-Hoc Networks. IXI Jornadas de Paralelismo (JP'08).

A.3 Book Chapter

- J. Serna, J. Luna, R. Morales and M. Medina. Analyzing the trade-offs between security and performance in VANETs. Accepted for Wireless Technologies in Vehicular Ad Hoc Networks: Present and Future Challenges. Ed. IGI-Global, March 2011.

A.4 Technical Reports

- Serna, J., Luna, J., Medina, M.: A Survey of Security, Trust and Privacy for Vehicular Ad-Hoc Networks. REF: UPC-DAC-RR- XCSD-2008. UPC (2008).

- Serna, J., Luna, J., Medina, M.: Trust Management and Privacy for Vehicular Ad-Hoc Networks. REF: UPC-DAC-RR-XCSD-2008-8. UPC Catalonia (2008).

References

Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R. & Leinmüller, T. (2006). Attacks on inter vehicle communication systems - an analysis. In *In Proc. WIT*, 189–194. 17, 22

Armstrong, L. (2012a). Dedicated short range communications (dsrc). http://www.leearmstrong.com/DSRC/DSRCHomeset.htm. 11

Armstrong, L. (2012b). Dedicated short range communications (dsrc). 91

Behrisch, M., Bieker, L., Erdmann, J. & Krajzewicz, D. (2011). Sumo - simulation of urban mobility: An overview. In *SIMUL 2011, The Third International Conference on Advances in System Simulation*, Barcelona, Spain. 87

Beresford, Alastair, R. & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, **2**, 46–55. 23

Blake-Wilson, S., Brown, D. & Lambert, P. (2002). Use of elliptic curve cryptography (ecc) algorithms in cryptographic message syntax (cms). http://www.ietf.org/rfc/rfc3278.txt. 85

Boneh, D. & Franklin, M.K. (2003). Identity-based encryption from the weil pairing. *SIAM J. Comput.*, **32**, 586–615. 27

Borsetti, D., Fiore, M., Casetti, C. & Chiasserini, C. (2009). Cooperative support for localized services in vanets. *International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems*. 65, 94

C2CCC (2012). Car to Car Communication Consortium. http://www.car-to-car.org/. 11

Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K. & Zwingelberg, H. (2012). Architecture for attribute-based credential technologies. 54, 55

Casola, V., Luna, J., Manso, O., Mazzocca, N., Medina, M. & Rak, M. (2007a). Interoperable grid pkis among untrusted domains: an architectural proposal. In *Proceedings of the 2nd international conference on Advances in grid and pervasive computing*, GPC'07, 39–51, Springer-Verlag, Berlin, Heidelberg. 43

Casola, V., Mazzeo, A., Mazzocca, N. & Vittorini, V. (2007b). A security metric for public key infrastructures. *Journal of Computer Security*, **15**. 35, 43

Casola, V., Mazzocca, N., Luna, J., Manso, O. & Medina, M. (2007c). Static evaluation of certificate policies for grid pkis interoperability. In *ARES*, 391–399, IEEE Computer Society. 32, 41

Chaum, D. & Heyst, E.V. (1991). Group signatures. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, 257–265, Springer-Verlag, Berlin, Heidelberg. 26

Choi, J.Y., Jakobsson, M. & Wetzel, S. (2005). Balancing auditability and privacy in vehicular networks. In A. Boukerche & R.B. de Araujo, eds., *Q2SWinet*, 79–87, ACM. 24

Committee, I. (2007). Ieee std 1609.3 - ieee trial-use standard for wireless access in vehicular environments. 1, 23, 85, 93

de Fuentes, J.M., González-Tablas, A.I. & Ribagorda, A. (2010). Overview of security issues in vehicular ad-hoc networks. In *Handbook of Research on Mobility and Computing. IGI Global*, 189–194. 17

Dötzer, F. (2005). Privacy issues in vehicular ad hoc networks. In *in Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks*, ACM Press. 16, 23

Fischer, L., Aijaz, A., Eckert, C. & Vogt, D. (2006). Secure revocable anonymous authenticated inter-vehicle communication (sraac). In *4th Workshop on Embedded Security in Cars (ESCAR 2006)*. 25

Fonseca, E., Festag, A., Baldessari, R. & Aguiar, R.L. (2007). Support of anonymity in vanets - putting pseudonymity into practice. In *WCNC*, 3400–3405, IEEE. 24

Gerlach, M. (2006). Assessing and improving privacy in vanets. In *4th Workshop on Embedded Security in Cars (ESCAR 2006)*. 23, 24

Gerlach, M. & Güttler, F. (2007). Privacy in vanets using changing pseudonyms - ideal and real. In *VTC Spring*, 2521–2525, IEEE Vehicular Technology Conference (VTC2007-Spring. 24

Gerlach, M., Festag, A., Leinmuller, T., Goldacker, G. & Harsch, C. (2007). Security architecture for vehicular communication. In *Proc. 5th Int'l Workshop on Intelligent Transportation (WIT)*. 93

Golle, P., Greene, D. & Staddon, J. (2004). Detecting and correcting malicious data in vanets. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 29–37, ACM, New York, NY, USA. 24

Guerrero-Ibez, A., Flores-Corts, C. & Damin-Reyes, P. (2012). *Development of Applications for Vehicular Communication Network Environments*, 183–204. Hershey IGI Global, PA, USA. 14

Guo, J., Baugh, J.P. & Wang, S. (2007). A group signature based secure and privacy-preserving vehicular communication framework. 26

Haas, J.J., Hu, Y.C. & Laberteaux, K.P. (2009). Design and analysis of a lightweight certificate revocation mechanism for vanet. In R. Shorey, A. Weimerskirch, D. Jiang & M. Mauve, eds., *Vehicular Ad Hoc Networks*, 89–98, ACM. 25

Housley, R., Ford, W., Polk, W. & Solo, D. (1999). X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol. 30

Housley, R., Ford, W., Polk, W. & Solo, D. (2002). Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile. 20, 31, 33

Hubaux, J.P., Capkun, S. & Luo, J. (2004). The security and privacy of smart vehicles. In *Security and Privacy, IEEE*, vol. 02, 49–55. 11, 22

Hui, L., Hui, L. & Zhanxin, M. (2010). Efficient and secure authentication protocol for vanet. In *Proceedings of the 2010 International Conference on Computational Intelligence and Security*, CIS '10, 523–527, IEEE Computer Society, Washington, DC, USA. 27

IEEE LAN/MAN Standards Committee – IEEE802 (2012). Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 12

Kargl, F., Ma, Z. & Schoch, E. (2006). Security engineering for vanets. In *ESCAR '06*. 16, 18

Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., Thong, T.V., Calandriello, G., Held, A., Kung, A. & Hubaux, J.P. (2008). Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications*, **46**, 110–118. 93

Liao, J. & Li, J. (2009). Effectively changing pseudonyms for privacy protection in vanets. In *Proceedings of the 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, ISPAN '09, 648–652, IEEE Computer Society, Washington, DC, USA. 24

Lin, X., Sun, X., han Ho, P. & Xuemin (2007). Gsis: A secure and privacy preserving protocol for vehicular communications. 27, 28, 93

Mahmoud Al-Qutayri, F.A.H., Chan Yeun (2010). In *Computational Intelligence and Modern Heuristics*. 28, 93

Martínez-Silva, G., Rodríguez-Henríquez, F., Cortés, N.C. & Ertaul, L. (2007). On the generation of x.509v3 certificates with biometric information. In *Security and Management*, 52–57. 85, 93

Mousavi, S.M., Rabiee, H.R., Moshref, M. & Dabirmoghaddam, A. (2007). Mobisim: A framework for simulation of mobility models in mobile ad-hoc networks. In *WiMob*, 82, IEEE Computer Society. 87

Moustafa, H., Bourdon, G. & Gourhant, Y. (2006). Providing authentication and access control in vehicular network environment. In *SEC*, 62–73. 26

Myers, M., Ankney, R., Malpani, A., Galperin, S. & Adams, C. (1999). X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol. 32, 33, 45, 94

NHTS (2006). Vehicle safety communications project. Tech. rep., National Highway Traffic Safety Administration, US Department of Transportation. 16, 85, 94

NS2 (2012). Network Simulator v2. 87

OCSP, E. (2011). EJBCA OCSP. 86

Papadimitratos, P., Gligor, V. & Hubaux, J.P. (2006a). Securing Vehicular Communications - Assumptions, Requirements, and Principles. In *Proceedings of 4th Workshop on Embedded Security in Cars (ESCAR)*, 5–14, Berlin, Germany. 22

Papadimitratos, P., Kung, A., Hubaux, J.P. & Kargl, F. (2006b). Privacy and Identity Management for Vehicular Communication Systems: a Position Paper. In *Workshop on Standards for Privacy in User-Centric Identity Management*, Zurich, Switzerland. 23

Papadimitratos, P., Buttyan, L., Hubaux, J.P., Kargl, F., Kung, A. & Raya, M. (2007). Architecture for secure and private vehicular communications. In *International Conference on ITS Telecommunications*, 1–6, IEEE Computer Society. 23

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger J., Raya, M., Ma, Z., Kargl, F., Kung, A. & Hubaux, J.P. (2008). Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communcations Magazine*, **46**, 100–109. 25

Papapanagiotou, K., F., M.G. & Panagiotis, G. (2007). A certificate validation protocol for vanets. *Globecom Workshops, 2007 IEEE*, 1–9. 26

Parno, B. & Perrig, A. (2005). Challenges in securing vehicular networks. 17, 22, 93

PATH (2012). Partners for Advanced Transportation TecHnology. http://www.path.berkeley.edu/. 12

Petit, J. (2009). Analysis of ecdsa authentication processing in vanets. In *Proceedings of the 3rd international conference on New technologies, mobility and security*, NTMS'09, 388–392, IEEE Press, Piscataway, NJ, USA. 85, 93

Pfitzmann, A. & Hansen, M. (2005). Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology. Tech. rep., TU Dresden. 23

Plossl, K., Nowey, T. & Mletzko, C. (2006). Towards a security architecture for vehicular ad hoc networks. *ARES '06*, 8. 15

Raya, M. & Hubaux, J.P. (2005). The Security of Vehicular Ad Hoc Networks. In *3rd ACM workshop on Security of ad hoc and sensor networks (SASN)*. 15, 17, 22

Raya, M. & Hubaux, J.P. (2007). Securing vehicular ad hoc networks. In *Journal of Computer Security (JCS) 15(1)*, 39–68. 16, 18, 93

Raya, M. & pierre Hubaux, J. (2005). The security of vanets. In *In VANET05, September 2*, 93–94. 82

Rebollo-Monedero, D., Forné, J., Solanas, A. & Martínez-Ballesté, T. (2010). Private location-based information retrieval through user collaboration. 60

RSA (2002). Rsa cryptography standard. www.rsa.com. 85

Sampigethaya, K., Huangy, L., Li, M., Poovendran, R., Matsuuray, K. & Sezaki, K. (2005). Caravan: Providing location privacy for vanet. In *ESCAR '05*. 24

Santesson, S. & Hallam-Baker, P. (2010). Ocsp algorithm agility. 85

Serna, J., Luna, J. & Medina, M. (2008). Geolocation-based trust for vanet s privacy. In M. Rak, A. Abraham & V. Casola, eds., *Proccedings of the Fourth International Conference on Information Assurance and Security, IAS 2008, September 8-10, 2008, Napoli, Italy*, 287–290, IEEE Computer Society. 78

Wex, P., Breuer, J., Held, A., Leinmueller, T. & Delgrossi, L. (2008). Trust issues for vehicular ad hoc networks. In *in 67th IEEE Vehicular Technology Conference (VTC2008-Spring*. 22

WHO (2012). Global status report on road safety 2012. Tech. rep., World Health Organization. 1

Xiaodong, L., Xiaoting, S., Xiaoyu, W., Chenxi, Z., Pin-Han, H. & Xuemin, S. (2008). Tsvc: timed efficient and secure vehicular communications with privacy preserving. *IEEE Transactions on Wireless Communications*, **7**, 4987–4998. 82

Xiaoping, X. & Jia, D. (2012). Lpa: a new location-based privacy-preserving authentication protocol in vanet. *Security and Communication Networks*, **5**, 69–78. 27

Zarki, M.E., Mehrotra, S., Tsudik, G. & Venkatasubramanian, N. (2002). Security issues in a future vehicular network. In *In European Wireless*, 270–274. 2, 13

Zeadally, S., Hunt, R., shyan Chen, Y., Irwin, A. & Hassan, A. (2010). Vehicular ad hoc networks (vanets): Status, results, and challenges. 13