On-siteDriverID: A Secure Authentication Scheme based on Spanish eID Cards for Vehicular Ad Hoc Networks

Authors: J. Sánchez-García, J. M. García-Campos, D. G. Reina, S. L. Toral, F. Barrero.

University of Seville (Spain)

Escuela Superior de Ingenieros. Avda. Camino de los Descubrimientos, s/n

41092 Sevilla (Spain)

email: jsanchez73@us.es, josgarcam@etsi.us.es, dgutierrezreina@us.es, storal@us.es, fbarrero@us.es

phone: +34 954 48 12 93; fax: +34 954 48 73 73

Corresponding author: S. L. Toral

On-siteDriverID: A Secure Authentication Scheme based of Spanish eID Cards for Vehicular Ad Hoc Networks

Abstract:

Security in Vehicle Ad Hoc Networks (VANETs) has been a topic of interest since the origins of vehicular communications. Different approaches have been followed as new security threats have emerged in the last few years. The approach of conditional privacy has been widely used as it guarantees authentication among vehicles but not revealing their real identities. Although the real identity of the vehicle can be traced by the authorities, the process to do that is time consuming and typically involves several entities (for instance road authorities that request the identification, license plate records bodies, a judge to allow revealing the identity associated to a license plate…). Moreover, this process is always subsequent to the detection of a road situation that requires knowing the real vehicle identities. However, in vehicular scenarios, authorities would beneficiate from knowing the real drivers' identity in advance. We propose in this paper On-SiteDriverID, a secure protocol and its application which allows authorities' vehicles to obtain drivers' real identities rapidly and on demand on VANET scenarios. Thus, authorities would be able to gather information about drivers and vehicles, allowing them to act in a safer and better manner in situations such as traffic control duties or emergencies. The obtained simulation results in real VANET scenarios based on real maps guarantee that in the 60-70% of cases the proposed On-SiteDriverID successfully obtains the identity of the drivers.

Keywords: PKI, Vehicular Ad Hoc Networks, Authentication, ID Card.

1. Introduction

New security threats have emerged in the field of communications networks due to the recent growth of mobile computing and the intensive use of the Internet. The birth of new communication paradigms like the Internet of things (IoT) envision a world full of connected devices capable of exchanging information through the Internet [1]. The communications among such mobile devices must be carried out in a secure way so the interlocutors taking part in it can trust each other by means of authentication mechanisms. It is also important to guarantee message integrity and confidentiality of the information exchanged.

In general computer networks, there are plenty off-the-shelf security resources that could be applied with affordable costs in order to provide authentication. Methods for authentication are often categorized as i) something known, such as a password, ii) something possessed, for instance an identity card or iii) something a person is, i.e. a personal characteristic like a fingerprint. Smart cards bring less security vulnerabilities than only-password based authentication, and also their security deployment is cheaper than biometrics. Smart cards are considered a two-factor authentication mechanism, which is based in something possessed, that is the card, and something known, a password [2]. Also, smart cards' cryptographic capacity and portability are two features that make them one of the most widely adopted authentication methods [3].

National Governments have promoted the use of this authentication method during the last decade, improving the existing identity (ID) cards to include an information security infrastructure for citizens. This is the case of Spain, where the personal ID card has become a smart card, named after *electronic ID* or eID from now on. The Spanish eID contains personal information within a microchip that can be used for information

security purposes. The Spanish government is constantly promoting the electronic use of ID cards and has been distributing the API for developing new services based on it [4]. In addition to these resources, it can also be found a complete public key infrastructure (PKI), which is based on the Spanish ID card. This infrastructure is enabled and managed by the General Directorate of Police, known in Spanish as *Dirección General de la Policía*, DGP from now on. A complete description of the PKI used in the Spanish eID can be found in [5]. This PKI makes use of X.509 certificates [6] and the Online Certificate Status Protocol (OCSP) [7]. Thus, the Spanish eID enables to any Spanish citizen to authenticate him against any service that requires identification, making use of its digital signature and also other security mechanisms. It is worth pointing out that the digital or electronic advanced signature is considered like the handwritten signature by the Spanish law.

Ad hoc networks [8], and also the broader concept of Internet of Things paradigm [9], require novel security mechanisms. These networks are susceptible of both common and brand-new security threats [10]. The infrastructure-less nature of ad hoc networks, the fact of every node acting as a router, the mobility and the use of wireless communications links are the main reasons of such new security threats. As mentioned in [11], it is difficult to ensure authenticity and confidentiality in ad hoc networks, but one way to establish secure communications in ad hoc networks is the use of authentication and certification services.

As occurs with routing protocols for ad hoc networks, there is not a perfect security solution for ad hoc networks that guarantees secure communications in every situation, so the solution highly depends on the scenario characteristics.

In this paper, the Spanish eID is used to develop On-SiteDriverID, a secure authentication scheme and its application for urban VANET scenarios. In those scenarios, the road authorities, for instance the police, may find useful to know the real identity of the driver before taking any action. The proposed security scheme is of high interest as improves security in VANETs, specifically in situations where a direct, on-site and on demand authentication mechanism is required by a road authority[1]. Our solution of using the eID to secure specific communications in V2V communications complements current approaches for securing VANETs.

The primary objective of On-SiteDriverID is the creation of secure VANET scenarios through a mechanism that allows authorities to easily and automatically obtain drivers' identities. This avoids involving other entities (such as a judge) in the driver identification process which would make it complex and time-consuming. Consequently, On-SiteDriverID has a user-centric design from the point of views of the authorities which get the drivers' identities easily, from the point of view of the drivers which identify themselves against the authorities smoothly. This is simply accomplished by running the application that implements On-SiteDriverID security scheme.

The main contributions of this paper are twofold:

- The design of On-SiteDriverID, a secure authentication scheme and its application for VANET road authorities, based on the already in use Spanish eID smart cards.
- The evaluation of the proposed On-SiteDriverID on simulated realistic VANET urban scenarios.

[1] We call "authority" in this paper to any public organization with authority in the domain of road traffic. Examples of these are the police, and other emergency bodies like firefighters and paramedics.

The paper is organized as follows. Section II describes the related work. Section III describes the Spanish eID card and its public key infrastructure implementation. Section IV describes the On-SiteDriverID application, its application scenario and its implementation. The simulations results of an urban scenario are presented in section V. Finally, some conclusions are drawn in the section VI.

2. Related work

Several works describe the challenges in the field of secure ad hoc networks and the requirements for adapting traditional security mechanisms to ad hoc networks [12], [13], [14]. In [13], it is stated that a combination of cryptographic mechanisms can prevent the majority of attacks in ad hoc networks. In [11], [15], [16] and [17] the authors propose cryptographic mechanisms based on Public Key Infrastructure, PKI from now on, for securing ad hoc networks.

Regarding security mechanisms for VANETs, it is clear that there is a need for the information to be secured [18], as the messages contain relevant information such as driving routes and timestamps. Revealing this information associated with drivers' identity could be used for malicious purposes.

In [19], it is stated that PKI is one of the most suitable options for securing VANETs. Both authentication and non-repudiation are essential for identifying vehicle drivers liable for certain actions such as car accidents or traffic infractions. Even so, the security hardware architecture in VANETs was conceived with two main in-vehicle devices: i) the event data recorder or EDR, for recording vehicles' critical data in emergency situations; and ii) a tamper-proof device or TPD, responsible for all the cryptographic operations and the storage of private keys and certificates.

In [19], the authors also propose a Vehicular Public Key Infrastructure or VPKI. In this approach, the Certificate Authorities (CAs) will issue public-private key pairs for each vehicle, and at the same time, each vehicle would have a list of anonymous, but certified, keys that change frequently and are like one-time keys. This will maintain the drivers' privacy in order to protect them from several threats, but at the same time has to allow the authorities to reveal the message's source, i.e. the vehicle, for driving liability purposes. This is known as conditional privacy or conditional anonymity in [18]**.** Usually the approval of a judge is required in order to reveal the real identity of the driver [19]; other approaches involve several entities in this process, such as [20], which defines a Tracing Manager for approving the search of real identities and the Membership Manager which performs the search of the real identity in a database.

As stated in [21], the authentication schemes using smart cards are one of the simplest and most convenient authentication methods for secure data communications in insecure network environments. In [22]**,** a protocol called PAAVE is described. This protocol uses smart cards for securing VANETs communications. In PAAVE, the vehicle firstly authenticates itself against a Road Side Unit (RSU) through a public key cryptography procedure in which the RSU shares with the vehicle a session key; the session key is shared by all the vehicles authenticated against the same RSU so they can read other vehicles messages anonymously, i.e. the RSU is the only entity that could know the real identity of the driver. However, the vehicle's real identity is limited to knowing the driving license to identify the driver/owner. PAAVE does not clarify if a person driving a vehicle, and not being the owner of it, could be identified.

The previous works [18]**,** [19] and [20] provide real identities of the vehicles in specific road events after the event occurred, in a time-consuming manner and usually in a

process that involves several entities participation. Also, these works do not provide driver's information, but about the vehicle identity and ultimately about the owner.

In Spain, there is the guarantee that every car driver will be carrying an identification smartcard with him whenever he is driving i.e. the Spanish eID.

The Spanish eID has been used previously to create secure communications over wireless communications technologies such as Near Field Communications (NFC) [23].

In this paper, we propose a smart card based secure authentication scheme for VANETs based on the Spanish electronic ID card. In some cases the fact of a road authority having access to the driver's eID before responding to a road situation could be an advantage. This is beneficial because they could deal with these situations in a safer manner by knowing this driver's useful information in advance. On-siteDriverID advances in the integration of the security mechanisms available within the Spanish eID into VANET communications.

To the best of our knowledge, there are no other works in this field which have followed this specific approach for straight, on demand and on-site authentication of a vehicle driver against authority vehicles using eIDs in VANETs.

3. The Spanish eID and its Public Key Infrastructure (PKI)

The Spanish eID, now on DNIe, is the official identification card used in Spain. It is compulsory for citizens over fourteen years old. This card is a personal and non-transferrable document issued by the Ministry of the Interior. Figure 1 shows the Spanish DNIe. The DNIe can be described discerning between its physical characteristics and the digital information contained in its chip.

Physically, DNIe is a polycarbonate card which follows the ISO 7816 standard for smart cards [24]. It includes personalized information such as a photograph, the holder's personal signature, among other personal information. Several security elements are included in the DNIe and can be classified according to their perception capabilities:

- First level (user perception): Holograms, kinegrams, iridescences, etc.
- Second level (perception using devices): reactive UV inks, micro writing, etc.
- Third level (laboratory perception): Biometric comparison.

Figure 1. (a) Front DNIe; (b) back DNIe

From the point of view of the data included inside DNIe chip, the information is divided into three different security levels, which are in read-only access. These levels are:

- Public zone (without restricted access): CA intermediate issuing certificate, holder public keys, component certificate.
- Private zone (access with a Personal Identification Number or PIN): Holder signature, authentication X.509v3 certificates and holder private keys.
- Security zone (only accessible through police equipment): Electronic information which is the same than that physically written, biometric data, and the device serial number.

The DNIe is considered a Secure Signature Creation Device (SSCD) according to the Common Criteria EAL 4+ in the protection profile CWA 14169 [25] certified by the ETSI, the RFC 3739 and the European directive 99/93/EC [26]. The PKI

implementation for the DNIe is based on the X.509 standard [27], and is issued and signed previously by a Certification Authority, CA from now on. The veracity of certificating relies on the CA, if the CA and its methods can be trusted, then the certificate will be also trusted.

The DNIe enables a holder signature certificate. The purpose of the signature certificate is to allow citizens to have the possibility of digitally signing transactions and documents, guaranteeing both message integrity and authorship. To get the signature certificate is necessary to insert the holder PIN over a trusted channel [25] with the SSCD. Each signed task has to be authorized by the DNIe holder since the advanced electronic signature in Spain is equivalent to the legal hand signature [28], [26]. Several DNIe data fields that should be highlighted are:

- Subject: the holder personal data.
- Issuer: DGP.
- Subject Public Key Information: RSA encryption with key length of 2048 bits.
- Validity Period: 30 moths.
- Certificate Signature Algorithm: SHA-256 with RSA Encryption and SHA-1 with RSA Encryption.

4. On-SiteDriverID application using the Spanish eID in VANETs scenarios

In this paper, we propose the application of the proposed On-SiteDriverID in urban scenarios, where public organizations with authority in the domain of road traffic are present. Examples of these organizations are the police, and other emergency bodies like firefighters and paramedics. These organizations, called *authority* from now on, deal with traffic situations every day such as traffic control, roadblocks, car accidents,

etc. These authorities may be either physically present in traffic situations, such as driving authority vehicles, or remotely using the communications infrastructure available such as Road Side Units (RSU). We apply the proposed On-SiteDriverID in two common VANET scenarios, vehicle-to-vehicle communications (V2V) and vehicle-to-infrastructure (V2I), which represent most of the situations where the proposed authentication protocol can be used. In the used VANET scenarios the authority vehicles will request directly and on demand drivers' real identities. Consequently, there are no intermediary nodes in our scheme.

4.1. On-SiteDriverID authentication scenarios

According to the VANET types of communications, we consider two typical VANET scenarios such vehicle-to-vehicle communications (V2V), which represent the situation when the authority is represented by an authority vehicle (e.g. a police vehicle) and vehicle-to-infrastructure communications (V2I), in the case the authority take actions in the traffic situation remotely by using the communications infrastructure (e.g. the RSUs). The proposed On-SiteDriverID can easily applied to those scenarios to provide authentication services.

a) Vehicle-to-Vehicle authentication

We consider a scenario in which there are several vehicles driving along the roads of an urban area. The map is represented as a directed graph in which the roads are edges and the vertices are intersections. There is a set of vehicles moving around the network, each one at a different speed and with different direction. In this scenario, we include several authority vehicles, i.e. police cars, patrolling the area. The authority will request a direct and on-demand authentication to some vehicles of the network while they are moving. For example, a police car could request a driver to authenticate in the case it is

suspicious of any road infraction. This scenario is depicted in Figure 2. An important feature is that both the authority and the driver are moving so the time during which the proposed On-SiteDriveID is run should be shorter than in the case of V2I case.

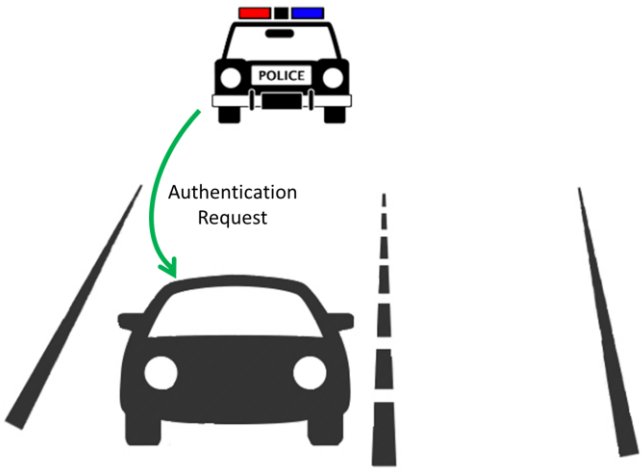

Figure 2. Vehicle-to-Vehicle authentication

b) Vehicle-to-Infrastructure authentication

In this scenario the authentication request is sent to driving vehicles from an authority body located in a fixed position. As an example, we can find this situation when a police vehicle is stopped on the road side and is requesting to the vehicles driving by to authenticate. Another example is when a traffic monitoring task is performed by a Road Side Unit (RSU) [29]. This scenario is depicted in Figure 3.

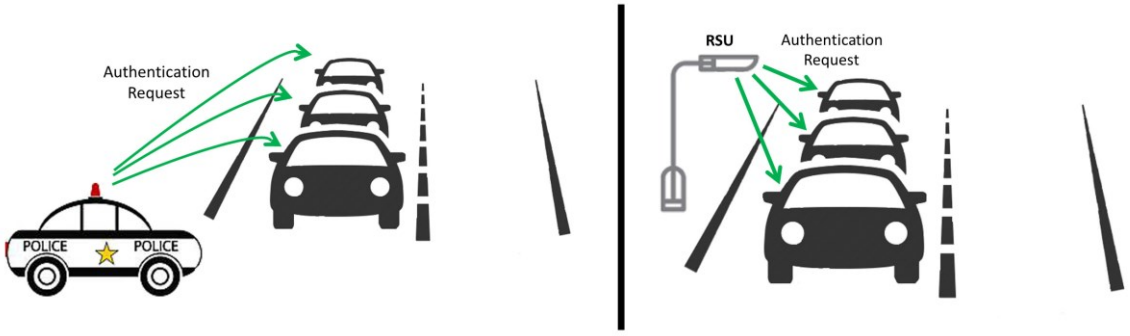

Figure 3. Fixed position and Vehicle-to-Infrastructure authentication

Vehicle-to-Infrastructure communications usually involve the communication between a vehicle and a RSU; however, as police vehicles performing traffic monitoring tasks can be also in a fixed static position close to the road, we have considered this situation as a V2I type.

4.2. Protocol description

We propose the following scheme to perform the identification of the real vehicle driver upon the request of an authority. To make a clear explanation of the On-siteDriverID scheme, we first introduce the data exchanged between the authority (represented by either an authority vehicle or an RSU) and the driver's vehicle.

The On-SiteDriverID authentication protocol consists of 4 messages exchanged between the authority and a driver's vehicle. These messages are depicted in Figure 4.

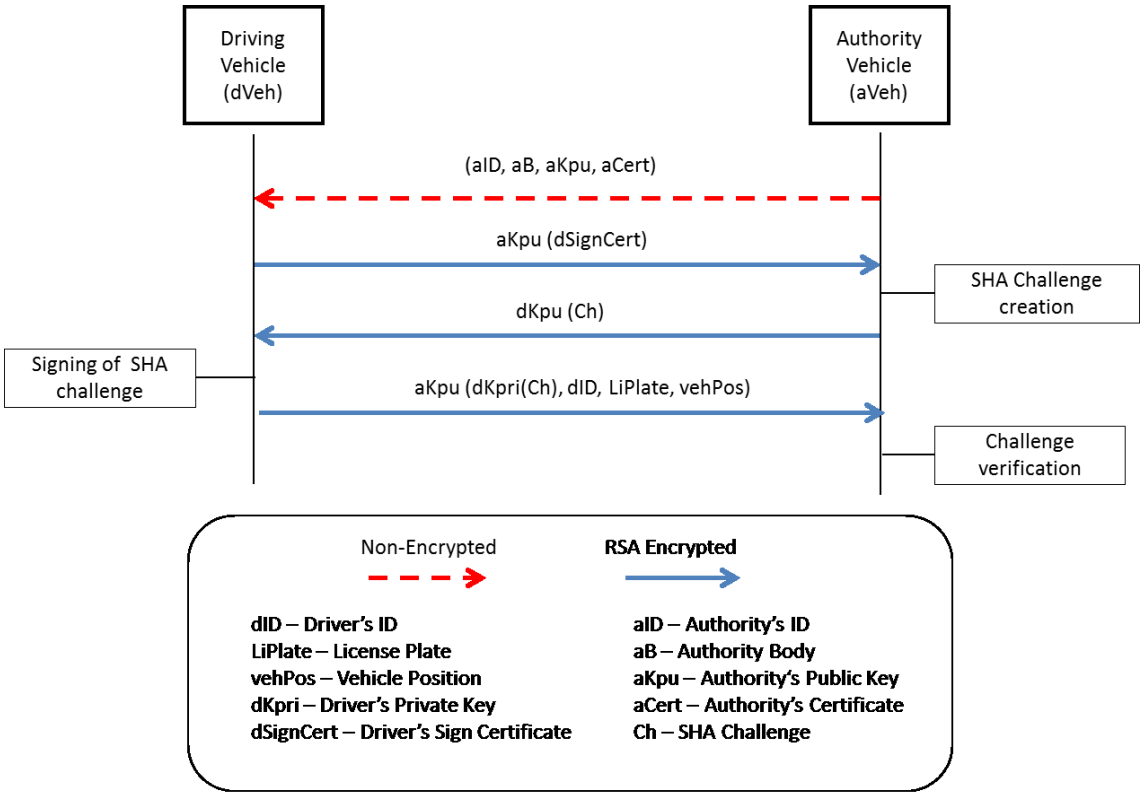

Figure 4. Messages Exchange for Driver Identification

Initially, the authority broadcasts a message called DIREQ (Driver Identification REQuest). Upon receiving a DIREQ message, a driver's vehicle will respond automatically with On-SiteDriverID protocol performed within the vehicle' TPD (tamper-proof device), in which the Spanish eID is integrated. Firstly, the TPD will check if the authority certificate is a valid one, i.e. whether the certificate is signed by a trusted party. In our implementations we trusted the certificates issued by the General Directorate of Police, as it is the same authority that issues the Spanish eID.

The driver's vehicle will respond to the DIREQ by broadcasting a message containing the sign certificate from the Spanish eID card. This certificate contains the driver's public key (dKpu) and also the sing of a third party guaranteeing that the dKpu belongs to the driver. In the case of the Spanish eID the Third Party is the Spanish General Directorate of Police. This message is sent encrypted with the authority's public key (aKpu), thus it is guaranteed that no one but the authority in question will be able to read the drivers certificate. This protects the driver's from bogus nodes aiming at impersonating an authority, as these will not be able to access the driver's certificate because they do not have the authority private key (aKpri) needed for the decryption.

The authority vehicle, receives the driver's sign certificate. Then, the authority generates a SHA-1 hash challenge, encrypts it with the dKpu and broadcasts it.

When the driver's vehicle receives the challenge message, decrypts it and signs it with its private key, dKpri. Then, the driver's TPD composes a message with the signed challenge and other non-signed information regarding the identity of the driver and the vehicle. This information consists of the driver's ID (dID), the vehicle license plate (LiPlate) and the vehicle location (vehPos). Eventually, the driver's TPD sings the entire message with the aKpu and broadcasts the message.

After receiving this information, the authority vehicle decrypts the message with its private key (aKpri) and decrypts the hash with the driver's public key (dKpu). If the challenge coincides with the one that the authority vehicle generated for this communication, then the authority can trust the ID of the driver, together with the license plate and the vehicle location. This protocol guarantees authentication and non-repudiation.

The messages exchanged in this protocol are composed of several fields. The first message's fields, also known as DIREQ or *message 0*, are described in Table 1. The size of the data fields have been calculated according to the requirements of the information to be transmitted. The aID field has a size of 63 bits, which yields from encoding with 7-bits ASCII the authority ID which is 9 characters long. The Authority Body data field is explained in Table 2. The Authority Certificate field size is of 1.5 kB, however depending on the information contained in the certificate the size could vary.

Data Fields	Description	Size
Authority ID (aID)	The proper identification of the authority e.g. the police agent badge number, or the police vehicle license plate.	63 b
Authority body (aB)	The authority organization e.g. Police, Health Services…	3 b
Authority' certificate (aCert)	A certificate issued by the Certification Authority which certifies the Authority's Public Key. In our case, it is considered the DGP (Spanish General Directorate of Police) as it is the same CA issuer of the Spanish DNIe.	1.5 kB

Table 1. DIREQ message or message 0 data fields

The Authority ID field is used in case it is needed to reveal the police agent that requested the identification of the driver. In Spain, the law enforcement bodies are obliged to carry their professional identification visible on their uniforms. This field acts as the visible authority identification number. Due to differences between several

bodies' professional identification numbers, this field has been represented using 9 alphanumeric characters, using 8 bits to represent each other (Extended ASCII).

In the Authority Body field (aB), 3 bits are used for identifying the entity that is behind the authentication request. In our implementation we mapped each number represented with these bits to a law enforcement organization or emergency services. Some codes are not used yet, and could be used in the future for other organizations using the On-SiteDriverID scheme.

Number	Authority Body	Description
000	National Police	Higher law enforcement body in Spain, mainly present in urban areas
001	Municipal Police	Law enforcement body with duties in municipal or local scenarios
010	Guardia Civil	Spanish law enforcement body actively involved in rural areas and highways traffic operations
011	Health Care Services	Public or private Health Care services bodies with ambulances present in the roads and aiding in car accidents
100	Military	Military forces
101	Future uses	-
110	Future uses	-
111	Future uses	-

Table 2. Authority Body field codes

The driver's vehicle responds to the DIREQ message with a message containing the driver's sign certificate. This message receives the name of *message 1*. The authority vehicle can extract from this certificate the driver's public key (dKpu). The fields of this message are described in Table 3. The Drivers' sign certificate field size is of 1.8 kB. As stated before, this is based on typical certificate sizes used on public Spanish authentication services such as the Spanish eIDs, but depending on the size of the certificate this file could vary.

Data Fields	Description	Size
Drivers's sign certificate (dSignCert)	The driver's Sign Certificate obtained from the Spanish eID. This certificate contains the driver's public key (dKpu) and a trusted third party sing for	1.8 kB

validation. This message is encrypted with the aKpu.

Table 3. Driver's sign certificate message or message 1

The message sent by the authority vehicle containing the SHA challenge is described in Table 4. This message is also known as *message 2*. The authority vehicle creates a SHA-1 hash challenge that must be signed by the driver's side in order to guarantee authentication and non-repudiation. The SHA-1 challenge field has been considered with a size of 192 bits as a result of the encryption of the SHA-1 challenge.

If this message is not received by the corresponding driver within the established time (Delay before the 1st retransmission, more details in next Section), it considers that the message was lost, and in consequence, the driver will send again the *message 1*. After two retransmissions, if the *message 2* is not received by the driver, it will discard the message and the procedure is finished.

Data Fields	Description	Size
SHA-1 Challenge (Ch)	A single per-session SHA-1 hash challenge created in the Authority side and encrypted with the dKpri.	192 b

Table 4. Authority challenge message or message 2

Finally, the message containing the driver's identity and related information is described in Table 5. This message receives the name of *message 3*. The Driver's ID field contains the personal ID number of the driver, which is unique. The TPD device will include also the vehicle License Plate in the message. The Vehicle Position field is included in order to provide more accurate information about the position of the vehicle. Eventually, the SHA-1 hash challenge signed with the dKpri. The dID field has a size of 63 bits which coincides with the ID size considered for authorities in Table 1. The License Plate field requires 35 bits which is the result of encoding the 4 numbers and 3 letters of a typical Spanish License Plate. The Vehicle Position field has a size of 32 bits due to the fact of using 32 bit decimal fixed point representation of the latitude and

longitude of the position. The SHA-1 Challenge field has a size of 192 bits as explained previously in Table 4. The total size of the message is 387 bits as a result of the addition of the previous data fields and the encryption with the aKpu.

When a *message 3* is not received by authority node, it uses the same technique employed in *message 2*, but in this case the authority node will retransmit the *message 2*. The time that the authority waits before retransmitting is named as Delay before the 2nd retransmission (more details are included in the next Section).

Data Fields	Description	Size
Driver's ID (dID)	The driver's identification number from the DNIe.	63 b
License Plate (LiPlate)	The License Plate of the vehicle, included in the TPD.	35 b
Vehicle Position (vehPos)	The vehicle position of the driver's vehicle.	32 b
SHA-1 Challenge (Ch)	The SHA-1 hash challenge encrypted with the dKpri.	192 b
TOTAL	The previous fields encrypted with the aKpu.	387 b

Table 5. Driver's identity message or message 3

Figure 5 shows a flow diagram which summarizes the proposed logic of the exchange of messages in the On-SiteDriverID protocol.

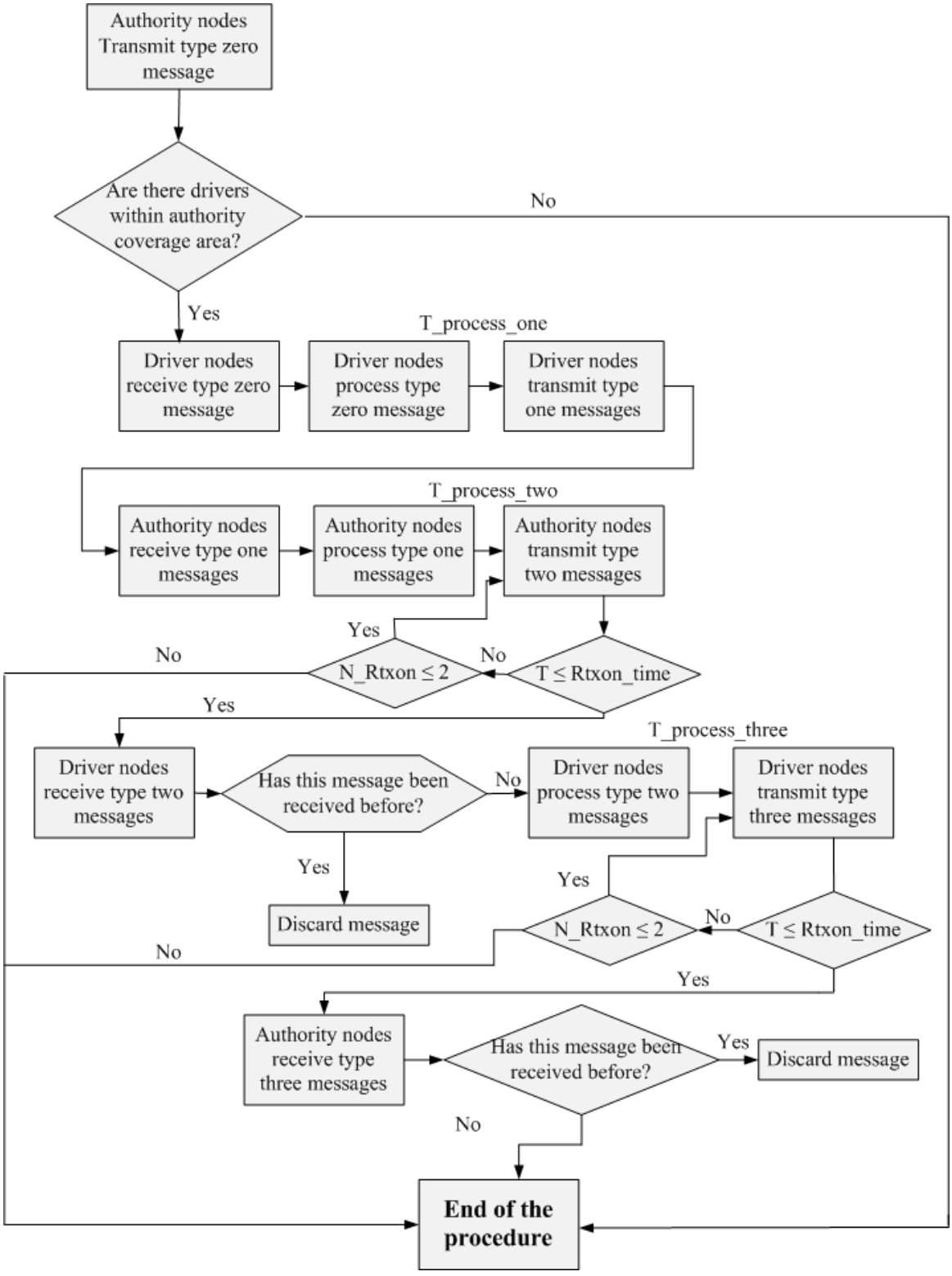

Figure 5 On-SiteDriverID Protocol Flowchart

5. Experimental results

This section presents the experiment results that validate the proposed On-SiteDriverID protocol. First, we show the implementation of a real prototype to be embedded in vehicles to easily use On-SiteDriverID. Second, we conduct a simulation study using VANET map-based scenarios.

5.1.On-SiteDriverID implementation prototype

We propose integrating an electronic device to the tamper-proof device (TPD) which enables the usage of the Spanish DNIe. This is used for securing the messages exchanged between the authorities' vehicle and other drivers in the aforementioned scenario.

We followed the communications architecture of a VANET defined in [29]. The communications equipment installed within a vehicle is called ITS vehicle station (Intelligent Transportation System), OBU (On-Board Unit) or OBE (On-board Equipment), depending on the standardization naming convention. The ITS vehicle station may be composed of different devices, namely an OBU router, an OBU host an OBU gateway. The implementation of the ITS vehicle station may differ from one vehicle to another depending on the type of vehicle and its applications. For example, in [29] three types of implementations are considered depending on the size of the vehicle. The definition of which devices compose the OBU is open to the vehicle manufacturer.

We propose a communication system similar to the OBU described in [30], but with some differences for the integration of the Spanish DNIe. The system that we propose is composed of two sub-systems, the *communication sub-system* and the *DNIe TPD*.

The main components of the *communication sub-system* are shown in Figure 6. These components perform as the OBU router module defined on the standards. These components are listed below:

- Alix3D3 Router Board
- MikroTik R52H 802.11AGB wireless network card
- 4GB CompactFlash card
- Dipole antenna dual 5GHz/2,4GHz 5 dBi

Figure 6. Alix3D2 with the MikroTik R52H wireless cards

In addition, the main components of the *DNIe TDP* are listed below. In our case the TPD is integrated with the OBU Host module defined on the standard:

- A Spanish DNIe
- DNIe card reader
- Raspberry Pi

It is important to note that in our system we have not implemented a whole TDP with a privacy-preserving scheme as the ones described in the related work section. Conversely, we have focused on the security provided by the On-SiteDriverID application in the target scenarios previously described.

Also it is worth to mention that the implementation of the secure device called as TPD in the literature has been partially implemented as part of the module called OBU Host in the standard [29]. This is due to the fact that the security services that are developed in typical VANET communications are a vertical block, which means that different security aspects can be implemented as different layers of the ITS communications stack and also to a different extent depending on the device.

The vehicle driver DNIe has to be inserted in the smartcard reader when the application is running in order to be able to respond to the messages requesting the real identity of the driver in the case a law enforcement vehicle requires it.

5.2. Simulation environment set up

Simulated scenarios

The proposed On-SiteDriverID has been implemented in a prototype with the aim of being installed in real vehicles. However, the evaluation of the proposed On-SiteDriverID in a real scenario is difficult since it requires a considerable amount of hardware investment and also the involvement of the authority organizations. In order to overcome these difficulties, simulation tools are a good alternative as they provide the possibility of defining scenarios according to specific features and simulate the performance of VANET applications on them.

The simulation framework used in this paper consisted in Citymob for Roadmaps (C4R) [31] for generating the mobility of vehicles in a road network. C4R is developed onto OpenStreetMap [32] tool, which gets the real roadmaps, and SUMO [33], which generates the vehicles' movements. The main features of the scenarios simulated are shown in Table 6. We select three different number of authority nodes to evaluate the proposed On-SiteDriverID protocol under different levels of congestion. Notice that the

higher the number of authority nodes, the higher the congestion. This is due to the fact that the number of authentication processes executed depends on the number of authority nodes. The chosen average speed is suitable for an urban scenario since in Spain the speed limit is fixed to 30 km/h in residential urban scenarios. The IDM mobility model [34] is widely used to emulate the movements of vehicles in urban scenarios. As a car-following model, the IDM describes the dynamics of the positions and velocities of single vehicles.

Feature	Description
Number of authority nodes	1, 4 or 9 depending on the situation
Number of driver's vehicles	100
Vehicles average speed	30 km/h
Simulation area	1000 square meters
Mobility model	Intelligent driver model (IDM) [34]
Map	Barcelona city (Spain)

Table 6. Main features of the simulated scenarios

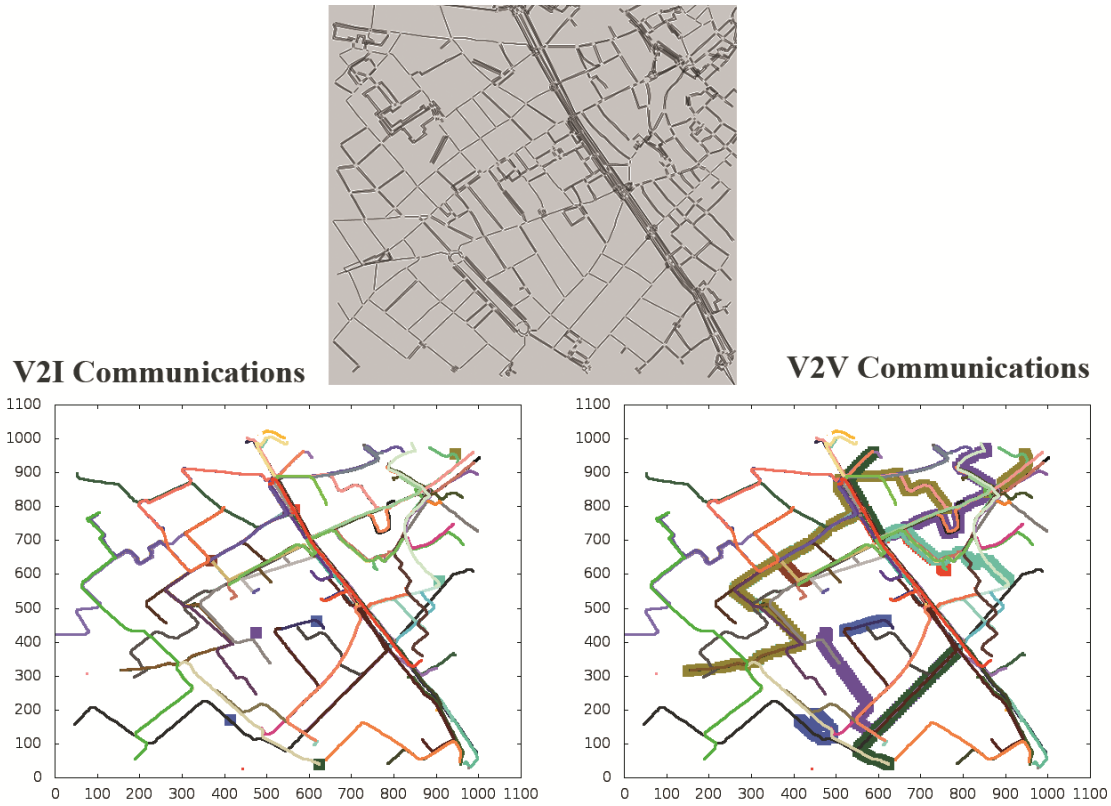

Figure 7 City layout and node movements

Figure 7 depicts the area of Barcelona, the one that has been used for the simulations. The top part of the Figure 7 is the model obtained from C4R; the left bottom part depicts the V2I communications and right bottom part the V2V communications. Each color that appears in Figure 7 represents a different node.

In order to simulate the communications and the exchange of messages among the authority and driver's vehicles in the simulated scenario, we have used the standard de-facto network simulation tool, NS-2 [35]. The main communications network characteristics are shown in Table 7. We use the IEEE 802.11p standard which is envisioned to be used in VANET scenarios according to Wireless Access Vehicular Environment (WAVE) suite standards. Regarding some design parameters of On-SiteDriveID protocols, we select the maximum number of retransmission as 2. Consequently, the authorities will try to retransmit the messages up to 2 times before considering that the vehicles are out of their radio transmission ranges.

Feature	Description
Access technology	IEEE 802.11p
Transmission range	250 m
Propagation model	Two-ray ground
Max. number of retransmissions if a message is lost	2
Delay before the 1st retransmission	20 seconds
Delay before the 2nd retransmission	40 seconds

Table 7. Main communications network features

The delay before the 1st retransmission has been chosen of 20 seconds. The reason for this is that the largest message processing time of the On-SiteDriverID is about 15 s. Consequently, it is reasonable to select a bigger delay than 15 s in order to avoid sending a retransmission during the time the other interlocutor is processing the received message. Moreover, the delay before the 2nd retransmission has been chosen double of the first delay. The reason for this selection is that in a real VANET the vehicles are moving and the time spent in a message to be received processed and sent

back again it is not only affected by the processing time, but it is affected by the location and speed of vehicles. Thus we chose 40 s in order to consider a largest delay that takes into account also the vehicle dynamics.

Performance metrics

In order to measure the effectiveness and performance of the On-SiteDriverID application, we used the metrics described in Table 8.

Metric	Description
Rate 1	The number of messages of type 1 received by the vehicles (either in the first transmission, the first retransmission or the second retransmission) divided by the total number of messages type 1 sent by the authorities.
Rate 2	The number of messages of type 2 received by the vehicles (either in the first transmission, the first retransmission or the second retransmission) divided by the total number of messages type 2 sent by the authorities.
Rate 3	The number of messages of type 3 received by the vehicles (either in the first transmission, the first retransmission or the second retransmission) divided by the total number of messages type 3 sent by the authorities.
Completed	The number of successfully completed processes of the On-SiteDriverID application divided by the total number of processes started. A successful completion of the process means that the authority vehicle has been able to authenticate the driver's ID.

Table 8. Performance metrics measured during the simulations

Simulation results

The proposed metrics have been measured for two different situations. On the one hand, communications between vehicles and the infrastructure (V2I), where the authority gets the identity of the driver's through the road infrastructure such as the RSUs (see Figure 8). On the other hand, communications between vehicles (V2V), where the authority is represented by the authority vehicle driving along the roads (see Figure 9).

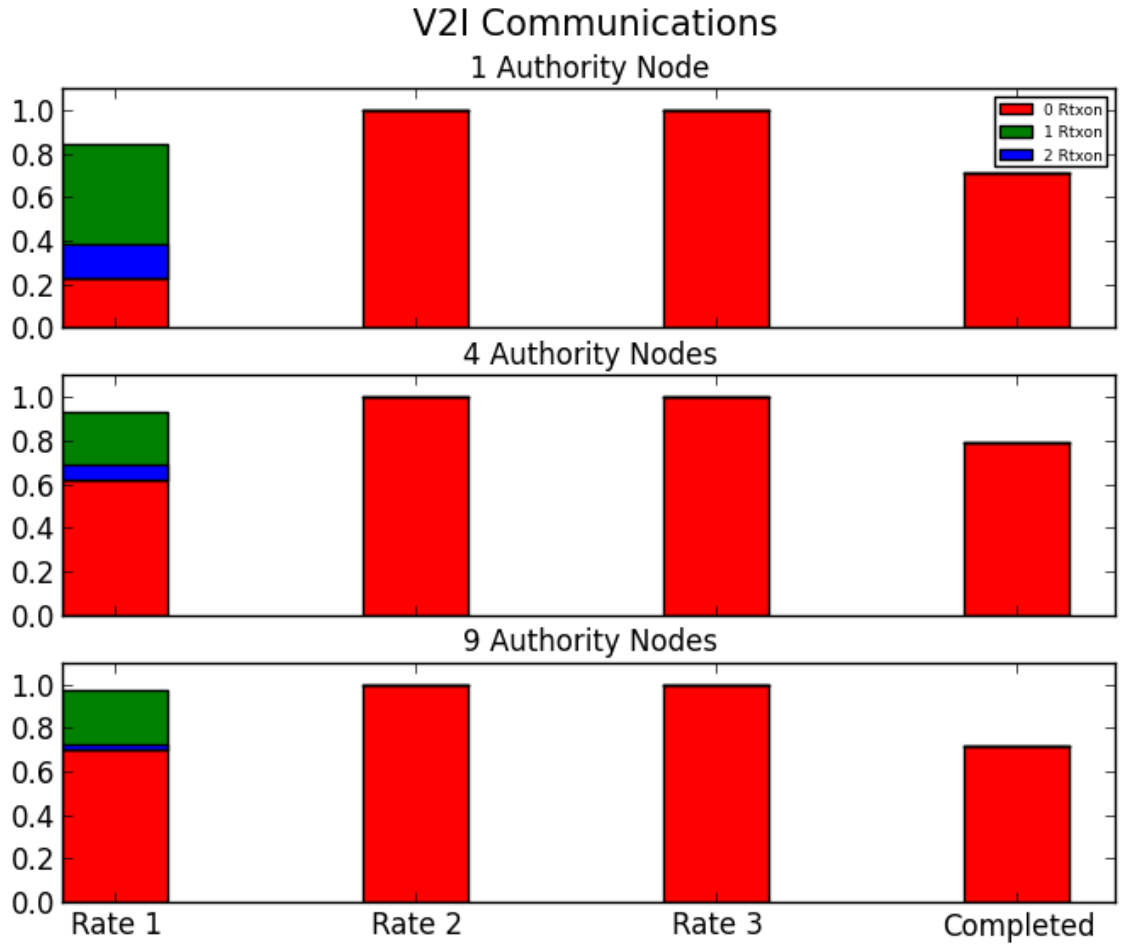

Figure 8 Simulation results for V2I Communications

The obtained results are promising since more that 70% of the processes, started by the authority, are successfully completed. The retransmission policy implemented by the OnSiteDriveID protocol is suitable for ensuring a higher number of successful processes. As we can see in Figure 8, messages of type 1 are the only ones that suffer from unsuccessful delivery to the receivers and, consequently, they need of first retransmissions (green color) and second retransmissions (blue colors). This is obvious because at the time of starting a process there are vehicles that are located on the edge of the transmission range of the authority (RSU) and are moving away of the authority. Thus, the first message can be received but as the driver's vehicle is not within the

transmission range of the authority vehicle, the police could not receive the message of type 1, and consequently there is the need of retransmissions.

The messages of type 2 and 3 do not suffer from retransmissions as we can see in Figure 8. This could be mainly related to the fact that if the authority is able to receive the message of type 1 from a driver's vehicle directly probably is because the authority (the RSU) and the driver are close enough to each other to complete the whole process without retransmissions.

V2I Communications								
		Transmited				**Received**		
1 Authority Node		**Message Type**				**Message Type**		
		1	**2**	**3**		**1**	**2**	**3**
		Nº Messages				**Nº Messages**		
	0 Retransmission	14	12	10		13	12	10
	1 Retransmission	11	0	0		3	0	0
	2 Retransmissions	3	0	0		3	0	0
4 Authority Nodes		**Message Type**				**Message Type**		
		1	**2**	**3**		**1**	**2**	**3**
		Nº Messages				**Nº Messages**		
	0 Retransmission	33	29	26		18	29	26
	1 Retransmission	15	3	0		9	0	0
	2 Retransmissions	6	3	0		2	0	0
9 Authority Nodes		**Message Type**				**Message Type**		
		1	**2**	**3**		**1**	**2**	**3**
		Nº Messages				**Nº Messages**		
	0 Retransmission	56	44	40		31	44	40
	1 Retransmission	25	4	0		12	0	0
	2 Retransmissions	13	3	0		1	0	0

Table 9. Summary of simulation results for V2I communications.

Table 9 summarizes the simulation results obtained for V2I communications, where it can be observed that the retransmission policy is also effective for the messages type 2. However, it is difficult to be noticed in the previous Figure 8.

The second situation, represented in Figure 9, corresponds to V2V communications. In this case the results are slightly worse than in the previous case. The main reason is that both nodes the authority and driver's vehicle are moving (in this case the authority is represented by a vehicle). Consequently, it is more difficult to successfully finish the four messages exchanges used by the proposed On-SiteDriverID.

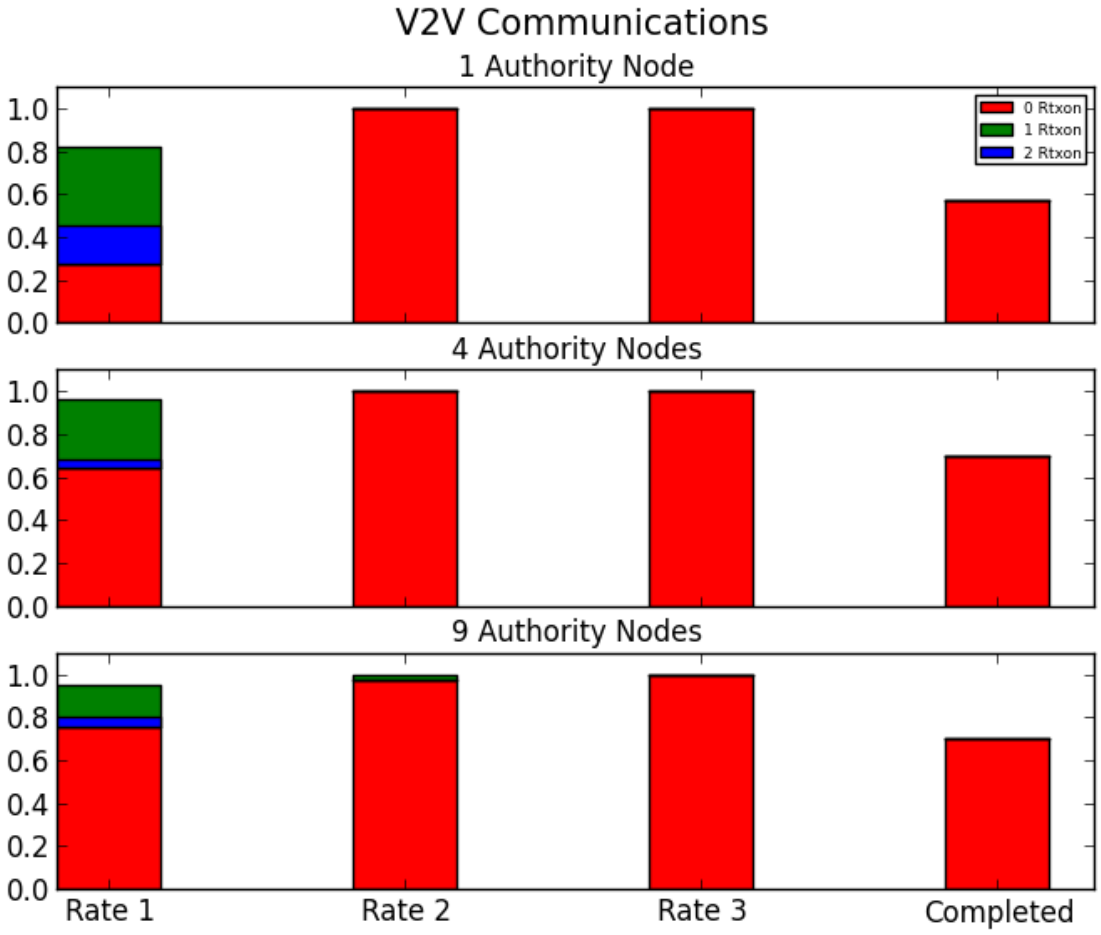

Figure 9 Simulation results for V2V Communications

However, the simulation results clearly show that about 60% of the processes started by the authorities are completed. Again, it is noticeable the role played by the

retransmissions that guarantee that more processes can be accomplished. Table 10 is included to provide more details about the simulation results.

V2V Communications								
		Transmited				Received		
1 Authority Node		Message Type				Message Type		
		1	2	3		1	2	3
		Nº Messages				Nº Messages		
	0 Retransmission	14	11	11		3	11	8
	1 Retransmission	11	3	0		6	0	0
	2 Retransmissions	5	3	0		2	0	0
4 Authority Nodes		Message Type				Message Type		
		1	2	3		1	2	3
		Nº Messages				Nº Messages		
	0 Retransmission	33	28	26		18	26	23
	1 Retransmission	15	5	0		9	0	0
	2 Retransmissions	7	5	0		1	0	0
9 Authority Nodes		Message Type				Message Type		
		1	2	3		1	2	3
		Nº Messages				Nº Messages		
	0 Retransmission	50	40	40		31	39	35
	1 Retransmission	19	5	0		8	1	0
	2 Retransmissions	12	5	0		2	0	0

Table 10. Summary of simulation results for V2V communications

6. Conclusions

We propose in this paper On-SiteDriverID, a secure protocol and its application which allows road authorities to obtain drivers' real identities on demand on VANET scenarios. This protocol and its application have been implemented using typical electronic devices used in a VANET integrated with the Spanish eID, which is the

device providing the secure identification of the driver against the road authorities. In order to get insights about the performance of the On-SiteDriverID application in a realistic VANET scenario, we have simulated the application running over a map of the city of Barcelona. The simulations have been developed on top of a set of software tools such as C4R (Citymob for Roadmaps) for the vehicles mobility generation and NS-2 for the network communications. We simulated two different VANET situations; the first one corresponds to 100 driver's vehicles driving while the authority gets the driver's identity remotely through the road infrastructure (RSUs), this represents a V2I communication in a VANET. In the second situation, the authority is represented by authority vehicles moving along roads, thus it corresponds to V2V communications. The obtained simulation results have shown that in the 60-70% of cases the proposed On-SiteDriverID successfully obtains the identity of the drivers. The remaining 40-30% of non-finished identification processes mainly correspond to vehicles that start the identification process but abandon the authority's coverage area during the process. As the authorities are mainly interested in the identity of drivers that are close to them we envision that a future direction of this work would be to implement a location-based mechanism in which only the vehicles closer to the authorities are required to provide their identities. This could be implemented by including the location of the authority in the first message and forcing the identification of drivers which are within a perimeter centred in the authority. Another option to increase the percentage of finished identification processes would be to make use of faster cryptographic algorithms such us Elliptic Curve cryptography (ECC). This will allow finishing the identification processes in shorter time, thus having a bigger amount of processes finished. The DNIe smartcard does not implement yet ECC algorithms; however we expect that the Spanish

entity that issues the DNIe (Dirección General de la Policía, DGP) will include them in future versions. Thus, authorities would be able gather the real identity of a bigger amount of drivers and vehicles, allowing them to act in a safer and better manner in road traffic situations.

Acknowledgements

This work was supported in part by the *Junta de Andalucía* through the contract of Jesús Sánchez García under the project P11-TEP-7555.

References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, «Internet of Things (IoT): A vision, architectural elements, and future directions», Future Generation Computer Systems, p. 1645–1660, 2013.

[2] M. Karuppiah and R. Saravanan, «A secure remote user mutual authentication scheme using smart cards» Journal of Information Security and Applications, pp. 282 - 294, 2014.

[3] T. Chen, H. Hsiang and W. Shih, «Security enhancement on an improvement on two remote user authentication schemes using smart cards» Future Generation Computer Systems, p. 377–380, 2011.

[4] Ministerio de Industria, Energía y Turismo, «Usa tu dni». Available: http://www.usatudni.es/dnie/.

[5] Dirección General de la Policía, Ministry of Interior, «Infraestructura de Clave Pública DNIe». Available: http://www.dnielectronico.es/PDFs/politicas_de_certificacion.pdf.

[6] R. Housley, W. Ford, W. Polk and D. Solo, «Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Technical report, RFC 2459:1999» 1999. Available: https://tools.ietf.org/html/rfc2459.

[7] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, «X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Technical report, RFC 2560:1999» 1999. Available: https://tools.ietf.org/html/rfc2560.

[8] V. Kärpijoki, «Security in Ad Hoc Networks» 2000. Available: https://www.cs.tcd.ie/hitesh.tewari/papers/netsec00_manet_sec.pdf.

[9] D. G. Reina, S. L. Toral, F. Barrero, N. Bessis and E. Asimakopoulou, «The Role of Ad Hoc Networks in the Internet of Things: A Case Scenario for Smart Environments» Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence, vol. 460, Springer Berlin Heidelberg, 2013, pp. 89-113.

[10] M. Renuka and P. Thangaraj, «Multi-path encrypted data security architecture for mobile ad hoc networks» National Conference on Innovations in Emerging Technology (NCOIET), Erode, Tamilnadu, 2011.

[11] Q. Chen, Z. M. Fadlullah, X. Lin and N. Kato, «A clique-based secure admission control scheme for mobile ad hoc networks (MANETs)» Journal of Network and Computer Applications, vol. 34, nº 6, p. 1827 – 1835, 2011.

[12] C. Zhang, M. Zhou and M. Yu, «Ad hoc network routing and security: a review» International Journal of Communication Systems, vol. 20, nº 8, pp. 909 - 925, 2007.

[13] P. Joshi, «Security issues in routing protocols in MANETs at network layer» Procedia Computer Science - World Conference on Information Technology, Istanbul, Turkey, 2011.

[14] K. T. Nguyen, M. Laurent and O. Nouha, «Survey on Secure Communication Protocols for the Internet of Things» Ad Hoc Networks, p. Accepted manuscript, 2015.

[15] S. Capkun, L. Buttyán and J.-P. Hubaux, «Self-Organized Public-Key Management for Mobile Ad Hoc Networks» IEEE Transactions on Mobile Computing, vol. 2, nº 1, pp. 52 - 64, 2003.

[16] S. Yi and R. Kravets, «MOCA : MObile Certificate Authority for Wireless Ad Hoc Networks» 2nd Annual PKI Research Workshop, Gaithersburg,MD,USA, 2003.

[17] L. Zhou and Z. Haas, «Securing Ad Hoc Networks» IEEE Network, vol. 13, nº 6, pp. 24 - 30, 1999.

[18] D. Antolino Rivas, J. M. Barceló-Ordinas, M. Guerrero Zapata and J. D. Morillo-Pozo, «Security on VANETs: Privacy, misbehaving nodes, false information

and secure data aggregation» Journal of Network and Computer Applications, vol. 34, nº 6, p. 1942–1955, 2011.

[19] M. Raya, P. Papadimitratos and J.-P. Hubaux, «Securing Vehicular Communications» IEEE Wireless Communications, vol. 13, nº 5, pp. 8 - 15, 2006.

[20] X. Lin, X. Sun, P.-H. Ho and X. Shen, «GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications» IEEE Transactions on Vehicular Technology, vol. 56, nº 6, pp. 3442 - 3456, 2007.

[21] M. Karuppiah and R. Saravanan, «A secure remote user mutual authentication scheme using smart cards» Journal of Information Security and Applications, vol. 19, nº 4 - 5, p. 282–294, 2014.

[22] V. Paruchuri and A. Durresi, «PAAVE: Protocol for Anonymous Authentication in Vehicular Networks Using Smart Cards» IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, 2010.

[23] J. M. León-Coca, D. G. Reina, S. Toral, F. Barrero and N. Bessis, «Authentication Systems Using ID Cards over NFC Links: the Spanish Experience using DNIe» Procedia Computer Science - The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013), 2013.

[24] International Standards Organization, «ISO 7816 - Identification cards - Integrated circuit cards» 2011.

[25] European Committee for Standarization (CEN), «CEN Workshop Agreement (CWA) 14169. Secure signature-creation devices "EAL 4+"» 2004.

[26] European Commission, «Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures» 2000. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML.

[27] International Telecommunication Union (ITU-T), «X.509 Recommendation: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks» 2012.

[28] Jefatura del Estado (Spanish Government), «Ley 59/2003, de 19 de diciembre, de firma electrónica» 2003. Available: http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399.

[29] European Telecommunications Standards Institute, «ETSI EN 302 665 v1.1.1 Intelligent Transport Systems (ITS); Communications Architecture» 2010-09.

[30] Z. Qin, Z. Meng, X. Zhang, B. Xiang and L. Zhang, «Performance evaluation of 802.11p WAVE system on embedded board» International Conference on Information Networking (ICOIN), Phuket, 2014.

[31] Grupo de Redes de Computadores, Universidad Politécnica de Valencia, «C4R: CITYMOB FOR ROADMAPS». Available: http://www.grc.upv.es/Software/c4r.html.

[32] «Open Street Map». Available: http://www.openstreetmap.org/.

[33] M. Behrisch, L. Bieker, J. Erdmann and D. Krajzewicz, «SUMO - simulation of urban MObility: an overview» Proceedings of the Third International Conference on Advances in System Simulation (SIMUL2011), Barcelona, Spain, 2011.

[34] M. Treiber, A. Hennecke and D. Helbing, «Congested Traffic States in Empirical Observations and Microscopic Simulations» Physical Review E, vol. 62, nº 2, pp. 1805-1824, 2000.

[35] «ns-2». Available: https://ant.isi.edu/nsnam/index.php/Main_Page.