UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- InfoRewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2010)

"Information Technology inTourism Industry"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 1, February 2010

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Authentication and Privacy in Vehicular Networks

José-María de Fuentes García-Romero de Tejada, Ana-Isabel González-Tablas Ferreres, and Arturo Ribagorda-Garnacho

Vehicular ad-hoc networks (VANETs) are composed mainly by vehicles. These communication networks allow data interchanging. In this way, more and better information is provided to drivers, thus achieving a better road safety. Information security is critical in these scenarios, as human lives are at stake. Particularly, spreading false data should be prosecuted, so sender identification and authentication is needed. However, it could allow vehicle tracking. In this way, privacy protection must also be achieved. In this work, mechanisms to fulfill this authentication-privacy compromise are analyzed.

Keywords: Authentication, Privacy, Pseudonym, VANET.

1 Introduction

Nowadays, road transport is a critical issue for the social and industrial activity in developed countries. For this reason, its efficiency and effectiveness is improving every day. In particular, road safety is a primary objective in transport policies of many industrialized countries. As an example, the *Vision Zero* Swedish project, <http://www.monash.edu.au/muarc/reports/papers/visionzero.html>, is intended to remove all traffic fatalities by 2020.

Simplifying drivers´ decision making is essential to improve road safety. In particular, one of the current problems in this area is the lack of global information from the driver point of view. He makes his decisions using available data, which is reduced to what lies within his field of vision. However, these data are often insufficient to make the optimal decision, that is, the one that provides maximum security for all vehicles. For example, if the vehicle ahead slows down, it would be interesting to know whether this is due to a slight adjustment of speed in a specific section or by the immediate occurrence of an accident. In both cases, drivers' actions should be different from the road safety viewpoint.

To help the resolution of this issue, a new kind of information technology called vehicular *network* or VANET (Vehicular Ad-hoc NETwork) is being developed. Thanks to this new type of network, vehicles become communication nodes that can share information about the status of its environment (e.g. pavement status, driving speed, accident warnings, etc.). By using these data drivers have more elements to steer vehicles more safely.

As a practical example of application developed on a vehicular network, the *eCall*, <http://www.esafetysupport.org/en/ecall_toolbox/>, project is intended to make the vehicle itself contact the emergency center when it is involved in an accident. Thus, assistance tasks are managed more efficiently, probably decreasing road traffic fatalities.

Vehicular networks are therefore a valuable integration of information technologies in the transportation area. However, there are numerous risks to be considered in these networks related to the management of vehicles' identities. In particular, on the one hand it is necessary to identify and authenticate participating vehicles (for liability purposes, among other things). But, on the other hand, privacy protection must also be achieved. In this work we will analyze the main mechanisms to authenticate a vehicle while adequately protecting its privacy. Before going into detail on this issue, the next section introduces how these networks are established and what type of information is at stake.

Authors

José-María de Fuentes García-Romero de Tejada is Computer Scientist and MSc in Computer Technology by the *Universidad Carlos III de Madrid*, Spain. He received the best academic record award in 2007. He is currently teaching assistant within SeTI (IT Security Research Group) of the Computer Science Department in the *Universidad Carlos III de Madrid*. He is working towards the PhD degree in the VANET security area. He has published several articles both in national and international conferences. <jfuentes@ inf.uc3m.es>

Ana-Isabel González-Tablas Ferreres is Associate Professor in the Computer Science Department at the *Universidad Carlos III de Madrid*, Spain. She is a Telecommunications Engineer by the *Universidad Politécnica de Madrid* (1999) and received her PhD degree in Computer Science from the *Universidad Carlos III de Madrid* in 2005. Her main research interests are security and privacy for location-based services and digital signature applications. <aigonzal@ inf.uc3m.es>

Arturo Ribagorda-Garnacho is a Telecommunications Engineer and holds a PhD in Computer Science from the *Universidad Politécnica de Madrid*, Spain. He is a Full Professor at the *Universidad Carlos III de Madrid*, leading its IT security research group. He has participated, and currently participates, in several national and European research projects. He has published numerous articles in national and international journals and conferences. <arturo@inf.uc3m.es>

2 Characterization of Vehicular Networks

In general, vehicular networks have two distinguishing

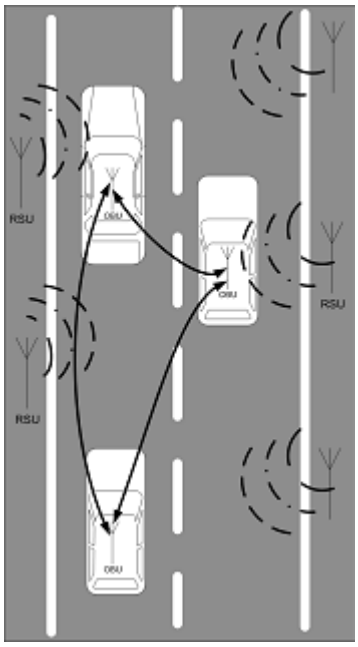

Figure 1: Typical Architecture of a Vehicular Network.

features compared with other traditional network scenarios. On the one hand, they cover a large geographical area, the road network. On the other hand, vehicles are moving at very high speeds. This mobility causes vehicular connections to be sporadic or *ad-hoc*. All these issues have led to the creation of a new communication technology, called DSRC (Dedicated Short-Range Communications, <http://www.leearmstrong.com/DSRC/DSRCHomeset.htm>). This technology can be defined as a variant of the existing wireless communication standard (802.11) in which sporadic short-range communications are established.

A vehicular network involves two types of entities, as reflected in Figure 1. On the one hand, most nodes are the vehicles themselves, which incorporate a communication device called OBU (On-Board Unit). In addition, a RSU (Road-Side Unit) is a stationary communication device that is placed along the roads.

These entities can establish two different types of communication. First, it allows interconnection between nearby vehicles. This makes possible the sharing of environment data previously introduced. Moreover, vehicles (through its OBU) and RSUs can get connected to exchange data to and from service providers that operate through vehicular networks. For example, this makes possible spreading traffic warnings sent by the Traffic Department.

3 Authentication-privacy Tradeoff in Vehicular Networks

Data exchanges described so far have several security requirements that must be satisfied. In fact, data security plays a crucial role in these networks. Since the received data can affect driving and therefore the passengers' safety, it is essential to ensure its accuracy. This is why it must be possible to pursue (and to isolate) those vehicles that spread false data.

Taking this into account, it is firstly desirable to have mechanisms to *identify* all vehicles. Secondly, it is necessary to *authenticate* such vehicles, that is, to assure that the vehicle is the one it claims to be. In this way, it will be possible to discover the vehicle that delivered a specific message and to apply the corresponding punishment (in case the message contains false information). For example, if a vehicle falsely announces a jam through the VANET, the sender should be identified in order to punish him.

However, this authentication must not violate the required *privacy* of all participants. If the vehicle inserts its identity in every message it sends, it would be possible *to track* its movement [1]. This is a problem as long as a relationship between a vehicle and its driver can usually be established. In fact, the vehicle's owner is its most common driver. Therefore, the vehicle identification becomes indirectly that of the driver or owner. In this situation, since tracking affects not only a vehicle but also a person, privacy protection must be achieved. This need is especially present in this scenario, as RSUs are generally maintained by the regional administration. In these circumstances, RSUs could allow monitoring all vehicular communications by this administration, replicating the "big brother" phenomenon on the road [2].

Vehicular networks face this *authentication-privacy tradeoff* from the depth of its essence. It is a central issue when designing and developing the network itself. For this reason, many research contributions have focused on mechanisms to meet this commitment. The objective is to have electronic credentials that attest its holder´s identity, without the chance of tracking or obtaining any sensitive data from its mere use. The main mechanism currently considered for identifying vehicles are temporary pseudonyms, using their associated public key certificates as credentials.

4 Identification of Vehicles

Currently, outside VANETs context, a vehicle is identified on two separate occasions. On the one hand, the manufacturer assigns a unique number (commonly known as *chassis number*) after the manufacturing process. On the other hand, an administrative permission should be obtained before putting the vehicle on the road – at least in Spain. This authorization means that the owner is registered as such and involves also the issuance of *license plates* to be placed in the vehicle.

Both identities are qualitatively different. In particular, chassis numbers do not change during vehicles' lifetime and they are located inside. However, license plates can be changed (e.g. after selling the vehicle) and they are designed to be viewed from outside.

Related to the problem of monitoring (and, by extension, of privacy) that must be avoided in vehicular networks, license plates are a common starting point for all future solutions – visual tracking is always possible if adequate means (e.g. cameras) are available [3]. For this reason, an electronic identification mechanism that provides perfect

anonymity would not be appropriate, as it may always be circumvented by physical means. In this situation, future contributions on this issue must provide at least the same level of privacy that exists today.

A natural extension of the described license plate has been proposed in the VANET context. It is called ELP (Electronic License Plate), a unique identifier issued by a legal authority [4]. However, using ELPs as permanent electronic identifiers would play against privacy. If employed in two messages delivered at different locations, both could be related and then vehicle tracking could be performed. This would make the existing privacy problem worse. Nowadays, this problem exists because an observer located aside the road can identify circulating vehicles in that road stretch. Using permanent electronic identifiers, this monitoring could be done remotely, in multiple places at once.

In this situation, other solutions to identify and to authenticate vehicles (or their messages) while protecting the privacy must be designed. The alternative that is receiving more attention in the literature are *pseudonyms* [5]. They are actually aliases that conceal the real identity. One way to implement them would be to use random numbers. Generally speaking, any technique that allows the legal authority to reveal the real identity associated with a pseudonym is valid. Otherwise, the liability requirement could not be fulfilled. On the other hand, if a vehicle uses the same pseudonym all the time, it would be easy to associate the alias with its real identity. To avoid this risk it is commonly assumed that a vehicle will use a different set of pseudonyms over time.

5 Creation of Electronic Credentials: Pseudonym-based Certificates

One of the most widespread mechanisms to allow electronic entity authentication is *public key certification*. A public key certificate is issued by a certification authority, and it attests that its public key belongs to the certificate holder. It also implicitly attests that the holder is the only entity that knows the corresponding private key.

Public key certificates consist of two main data: the holder´s identity and the associated cryptographic material. In vehicular networks different alternatives have been proposed to create each of them. Both issues are covered separately in the following sections.

5.1 Identity in the Certificate

As discussed above, most current proposals assume that the vehicle´s identity is represented by a temporary pseudonym. In this way, the identity contained within the certificate does not reveal any sensitive data from its holder. However, it should still be possible to link that pseudonym to a real identity in case of misbehavior. To prevent abuse of authority, separation of roles is often assumed. In this way, different entities must cooperate to perform the identity resolution process [6]. Thus, there are two different authorities – a *legal authority* and a *certification authority*. The first one registers all vehicles, allowing them to be on the road. It also issues license plates. The second one manages temporary pseudonyms and their corresponding certificates. Both entities are reflected in Figure 2, which also shows different data known by each entity. The legal authority knows the real identity of a vehicle and its owner. On the other hand, the certification authority knows which pseudonyms are assigned to each vehicle. Thus, both have to cooperate in order to discover the real identity of a driver. Thanks to this role separation, the chance of abuse of authority is minimized.

5.2 Creating Public and Private Keys

Besides the creation of pseudonyms, it is necessary to create public and private keys that enable authentication of the certificate holder in a VANET. Exceptionally, using identity-based cryptography, identifiers (pseudonyms, in this case) can be used as public keys [7]. Otherwise, both identity and keys must be created separately.

Two main alternatives have been proposed to generate keys: a centralized creation or a distributed one. In the centralized alternative, the whole process is delegated on the certification authority. Vehicles periodically contact it to get not only new certificates, but also their corresponding private keys. On the contrary, in the distributed alternative each vehicle generates all the cryptographic material [8]. When new certificates are needed, the chosen pseudonym and the public key are submitted to the certification authority. It will then create the corresponding certificate using both data.

Both alternatives are made possible thanks to a reliable component which is usually assumed to be in vehicles. It is called TPM (Trusted Platform Module) and provides both reliable storage and cryptographic capabilities [9]. In both alternatives, the TPM is used to store the cryptographic material. However, in the distributed version it has a greater responsibility, as it also is responsible for the creation of this material.

Comparing both alternatives, the distributed version offers considerable advantages. It is more scalable because part of the processing is done by vehicles. In addition, the private key never leaves the vehicle, resulting in a higher level of security. However, the proper functioning of the TPM is now more critical. If it were possible to alter this component, several vehicles could agree to a set of pseudonyms and keys. In such situation, different entities could obtain the same certificates and, as result, they would be indistinguishable.

6 Collection and Use of Certificates

6.1 Initial Collection: Update Process

Once created, pseudonyms are used for a short period of time. In fact, the best option would be to use them only once. It would make tracking very difficult to perform. To achieve this goal it is necessary to get new certificates periodically. An interesting solution is to take advantage on the manufacturing and administrative authorization processes

to load an initial set of certificates on vehicles. Subsequently, new certificates could be loaded when technical inspections of vehicles are performed.

6.2 Policies for Pseudonym Change

The process of pseudonym change cannot be done arbitrarily. It is necessary to find a suitable time to perform the pseudonym change in order to provide an adequate protection of privacy. Consider a road stretch on which only two cars are running. If only one of them performs the pseudonym change, it would be useless – any outside observer can deduce that the new pseudonym belongs to the vehicle that changed it.

Taking this issue into account, several pseudonym change policies have been proposed so far. For example, one alternative is to *change it according to the speed* [5]. Under this policy, the faster the vehicle drives the higher rate of pseudonym change. This gives further uncertainty, even if the observer covers a long road stretch.

Moreover, random silent periods (i.e. time intervals in which no messages are sent) have also been proposed [10]. This makes it difficult for a third party to guess when the change will be performed. However, it is desirable to match those periods with those of other vehicles. Otherwise, no benefit will be achieved and the situation would be the same as in the starting example. To address this issue, previous contributions have focused on the creation of *mix contexts* [11]. These are areas where no communication infrastructure (i.e. RSUs) is placed aside the road. Therefore, mix contexts are unmonitored areas. When a vehicle enters in that context, it stops all its communications. Thus, if multiple vehicles are in that area at the same time, it is complex for an observer to continue tracking them when they leave the mix context.

The described policies for pseudonym change are only effective if such pseudonym is the only means of identification. In other words, if there are other factors that identify electronically the vehicle, using pseudonyms will not bring any advantage in terms of privacy protection. It should be noted that the vehicular network is designed as a protocol stack, each one providing different services. Each stack layer requires a different identifier, so a pseudonym change requires a coordinated change of such identifiers to be really effective [12].

However, even taking this issue into account, there are some inherent features of communication devices (i.e. OBUs) that can be employed to identify them. An example is the radio frequency fingerprint, an electromagnetic pattern that is maintained in all messages sent by a transmitter [13]. This feature must be taken into account for the assessment on the effectiveness of such pseudonym change mechanisms.

7 Revocation of Certificates

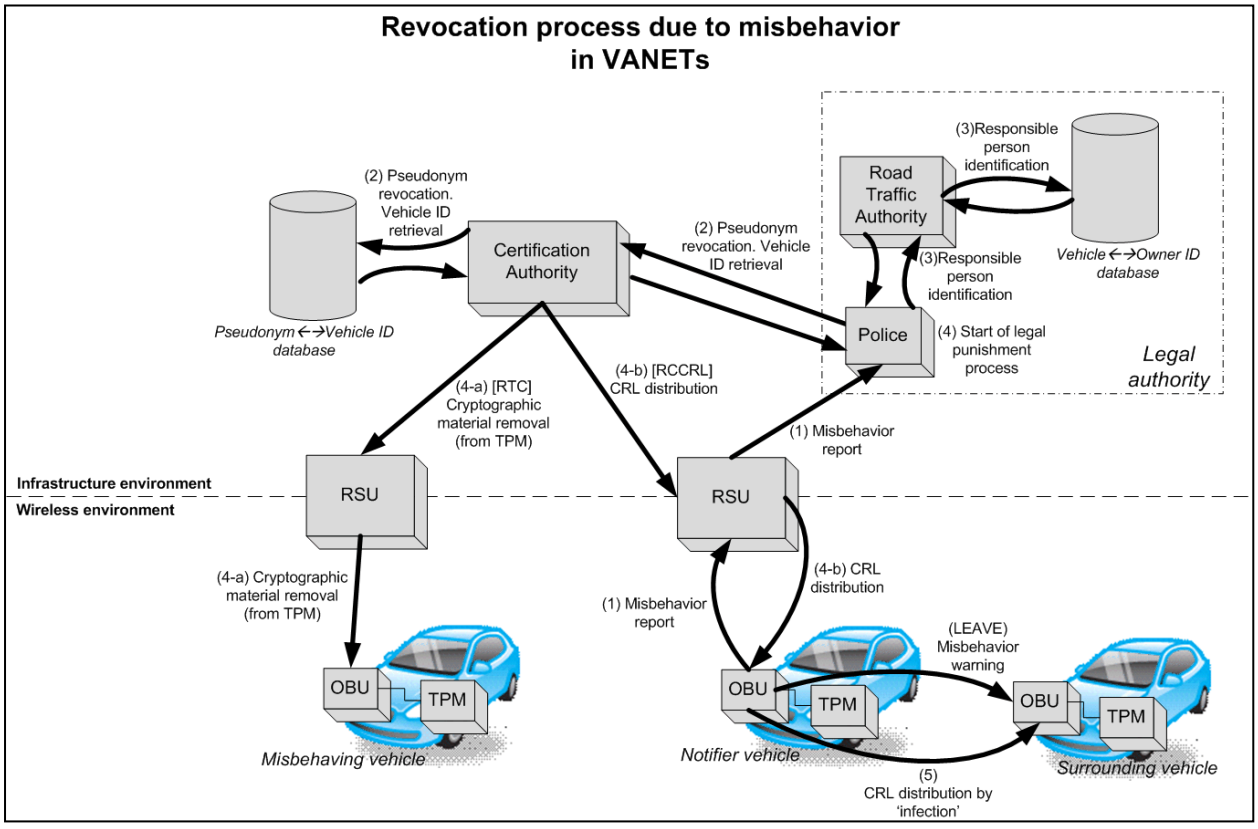

Figure 2: Revocation Process due to Misbehavior.

The identity management procedure involves not only its creation but also its revocation when necessary. The revocation procedure should be started when all the confidence on a given identity has been lost. This happens usually when the owner has lost control over the associated private key – in case of theft or loss, for example. Additionally, in this context the misbehavior of a vehicle in the network operation may be cause for revocation.

To illustrate this, let us introduce two examples of this bad behavior. First, consider a car which reports a false accident in order to simulate a situation of heavy traffic and thus obtain a free way. On the other hand, suppose that a vehicle does not take part in the message routing over the network. Both issues affect the normal VANET operation and therefore should be avoided. Revocation is the first defense mechanism and allows vehicles to isolate dishonest ones.

The above examples illustrate the two main phases of a revocation process: misbehavior *detection* and the corresponding *defensive* actions. The following sections examine each one separately. Figure 2 graphically describes the full revocation process. It will be explained in detail in the following paragraphs.

7.1 Misbehavior Detection

The detection of improper behavior is strongly conditioned by the nature of vehicular networks and, more specifically, by the way identity is managed in this scenario. As described so far, there is an entity that manages the certificates used to identify and authenticate each vehicle. However, there is no scalable way for vehicles to know with anticipation some data about others. This would be relevant, for example, to establish the confidence level on data reported by another vehicle taking into account its earlier behaviors. Thus, it is not possible to build a global model for managing the reliability (or reputation) that deserves a particular vehicle. In fact, it would not be efficient for each vehicle to store the reputation of all other vehicles – each vehicle will only encounter with a small amount of them and for a short time interval. A centralized reputation management cannot be implemented either, as the own nature of vehicular networks does not assume a permanent connectivity to outside entities.

In these circumstances, misbehaviors are identified locally and independently by surrounding vehicles. Proposed mechanisms are based on *plausibility checks*, that is, measuring the consistency of the data provided by a vehicle with respect to other claims made by others and its own sensorial knowledge [17].

7.2 Defensive Actions against Misbehavior

Once an inappropriate behavior has been detected, defensive actions should be progressive. A specific incorrect piece of information sent by a vehicle may not lead to a complete loss of confidence on it. A gradual isolation scheme based on the misbehavior persistence has been proposed [14]. This scheme is implemented through the LEAVE protocol. It proposes a voting system involving vehicles driving around the potential misbehaving one. Once the inappropriate behavior has been detected voters sent warnings to other vehicles (Figure 2). If the malicious behavior persists, they notify the legal authority to revoke the identity (Figure 2, message 1). One important issue is that only the authority can revoke the identity of any vehicle.

Once the revocation of a vehicle´s certificate has been decided, the first step is to contact the authority that manages pseudonyms to resolve the identity of the involved vehicle (Figure 2, message 2). Furthermore, its owner´s identity must be also revealed in order to process administrative notices that may arise (Figure 2, message 3).

From that moment on, the revocation itself must take effect. For this purpose, two different procedures can be used. First, the RTC protocol (Revocation of the Trusted Component) makes the authority contact directly with the reliable component (i.e. TPM) of the vehicle [14]. Recall that this component stores the vehicle's identity that must be now revoked. The authority sends a command that instructs the TPM to delete all identities (pseudonyms) of the vehicle, along with their associated cryptographic materials (Figure 2, message 4-a). To avoid spoofing attacks (i.e. an entity other than the certifying authority acting on behalf of it) the command is signed by the authority and the TPM verifies such signature before performing the required deletion. RTC is an effective solution but requires two preconditions. First, the current location of the vehicle whose identity is to be revoked must be known. Otherwise, the revocation command should be sent to all RSUs simultaneously, which would seriously affect the overall network performance. Second, it needs a reliable communication channel between the authority and vehicles. In fact, if an attacker is able to intercept that channel, RTC cannot be employed.

For those cases in which RTC cannot run, it is necessary to distribute the revocation information to other vehicles (Figure 2, message 4-b). However, there are many vehicles and they also can have multiple identities (pseudonyms). For this reason, traditional techniques for managing and distributing Certificate Revocation Lists (CRLs) are not suitable for the vehicular environment.

There are two proposed complementary alternatives for distributing CRLs. First, applying *compression* mechanisms to the whole list has been proposed [14]. This compression is done using a probabilistic tool called Bloom filters. It allows characterizing a group in such a way that it is possible to know with high probability whether an element is contained in it. Thanks to filters, data to be included in the revocation list is greatly reduced. Moreover, the CRL is divided into several pieces, simplifying its distribution. Each piece is individually verifiable, thus ensuring the authenticity of the contained data.

The second alternative for the CRL distribution is based on the biological process of epidemics [15]. Each vehicle that receives the updated revocation data becomes a carrier. When it meets other vehicles that do not have these data, it

infects them (Figure 2, message 5). This method exploits the potential of inter-vehicular communications, thus decentralizing the distribution itself.

8 Providing Private Non-repudiation of Origin

In some applications of vehicular networks it is necessary to ensure that the sender of a message cannot deny having sent it. This requirement, called non-repudiation of origin, is normally fulfilled using digital signatures. This is the same mechanism employed in applications that require a message (e.g. an accident warning) to be endorsed by several entities in order to be credible. However, using a traditional digital signature for this purpose, employing the vehicle´s permanent identifier, would be against its privacy – two messages signed by the same vehicle could be linked. Again, the problem of monitoring would be possible. Group signatures have been proposed in vehicular networks to contribute to solve this issue [8]. Essentially, this is a kind of signature in which the verifier can check that the message comes from a group member. However, the sender identity is not disclosed within the regular verification process. Only an authorized entity (generally the legal authority) might reveal the signer identity.

Group signatures have several underlying procedures that are very similar to those already described for managing pseudonym-based certificates. However, a substantial difference is that the creation of the public-private key pair cannot be distributed. This is because it is the certifying authority who establishes a set of parameters to create these keys. This creation process enables privacy on the signature verification process.

There exists an inherent threat in group signatures, which is commonly called as Sybil attack. In this attack, a single node uses multiple identities at the same time. Thus, it could sign the same message several times under different identities (for example, to endorse a traffic warning) and the receiver could not know whether these signatures come from different entities. There are two mechanisms to avoid this threat in vehicular networks. First, the trusted component itself provides security in this issue because it stores all that sensitive data. In this way, it is not possible to use multiple identities simultaneously. On the other hand, Message-Linkable Group Signatures have been recently proposed [16]. This mechanism ensures that, given two digital signatures on any message, the verifier can decide whether they are from two separate entities keeping their anonymity. As in the previous case, the authorized entity can reveal the signer identity.

9 Conclusions

Vehicular networks are a new and promising framework for new applications that will improve traffic management and road safety. However, multiple abuses can take place within these networks. For example, a vehicle could distribute false information through the network, confusing other vehicles. On the other hand, an observer could trace the path of a vehicle, compromising the privacy of its driver and occupants (if there is a way to know their identities).

All these issues highlight the need for a proper identity management, the creation of mechanisms to authenticate participants, and the protection of their privacy. In fact, these are critical issues in the development of vehicular networks and should be addressed at first. The solution of these problems will help to find a satisfactory evolution of these new networks.

In this work we have reviewed the main mechanisms to authenticate a vehicle while adequately protecting its privacy. We have focused on pseudonym-based public key certificates, as it is the most widespread alternative. Moreover, its revocation process has been also discussed, describing its problems and associated mechanisms. Finally, we have introduced some techniques to provide non-repudiation of origin in this area, again respecting the due privacy.

Acknowledgments

This work is partly funded by the Spanish Ministry of Science and Innovation, within the National Plan for Scientific Research, Technologic Development and Innovation 2008-2011, under contract TIN2009-13461 (project E-SAVE).

References

[1] Gerlach, M. (2005). VaNeSe - An approach to VANET security. V2VCOM.

[2] Raya, M., Hubaux, J.-P. (2005). The Security of Vehicular Ad Hoc Networks, Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), ACM.

[3] Parno, B., & Perrig, A. (2005) Challenges in Securing Vehicular Networks. Workshop on Hot Topics in Networks (Hotnets-IV).

[4] Hubaux, J.-P., & Capkun, S. (2004). The security and privacy of smart vehicles. IEEE Security and Privacy magazine, 2 (3), 49-55.

[5] Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. IEEE Wireless Communications, 13 (5), 8-15.

[6] Lin, X., Sun, X., Ho, P.-H., & Shen, X. (2007). GSIS: A Secure and Privacy-Preserving Protocol for vehicular communications. IEEE Transactions on vehicular technology, 3442-3457.

[7] Sun, J., Zhang, C., & Fang, Y. (2007). An ID-Based framework achieving privacy and non-repudiation in vehicular ad-hoc networks. Military Communications Conference (MILCOM) (pp. 1-7). Orlando, Florida, USA: IEEE.

[8] Callandriello, G., G. Papadimitratos, P., Lloy, A., & Hubaux, J.-P. (2007). Efficient and Robust Pseudonymous Authentication in VANET. International Workshop on Vehicular Ad Hoc Networks (pp. 19-28). Montreal, QC, Canada: ACM.

[9] Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., & Raya, M. (2007). Architecture for Secure and Private Vehicular Communications. 7th In-

ternational Conference on ITS, (pp. 1-6).
[10] Sampigethava, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2006). CARAVAN: Providing Location Privacy for VANET. International workshop on Vehicular ad hoc networks. ACM.
[11] Gerlach, M. (2006). Assessing and Improving Privacy in VANETs. Workshop on Embedded Security in Cars (ESCAR).
[12] Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure Vehicular Communication Systems: Design and Architecture. IEEE Communication Magazine.
[13] Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications Magazine, 46 (11), 110-118.
[14] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., & Hubaux, J.-P. (2007). Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, 25 (8), 1557-1568.
[15] Laberteaux, K. P., Haas, J. J., & Hu, Y.-C. (2008). Security Certificate Revocation List Distribution for VANET. International Conference on Mobile Computing and Networking (pp. 88-89). ACM.
[16] Domingo-Ferrer, J., & Wu, Q. (2009). Safety and privacy in vehicular communications. Lecture Notes in Computer Science, 173-189.
[17] Ostermaier, B., Dötzer, F., & Strassberger, M. (2007). Enhancing the security of local danger warnings in VANETs - a simulative analysis of voting schemes. International Conference on Availability, Reliability and Security. (pp. 422-431).

