# Geolocation-based Trust for Vanet's Privacy

Jetzabel Serna[1], Jesus Luna[2] and Manel Medina[1]

[1]Technical University of Catalonia, Computer Architecture Department,
Jordi Girona 1-3, D6-116. Barcelona 08034, Spain
*{jetzabel, medina}@ac.upc.edu*

[2] Barcelona Digital Technology Centre,
Sancho de Avila 110. Barcelona 08018, Spain
*jluna@bdigital.org*

***Abstract***: Research in Vehicular Ad Hoc NETworks (VANETs) has evolved considerably over the last years. Security and privacy in VANETs have recently appealed special interest in the research community. In this paper we overview the main privacy concepts and explain why these are fundamental for wide adoption of VANETs. Then, a set of privacy requirements for VANETs is established and studied towards proposing a novel mechanism beyond the use of pseudonyms. In particular, this research demonstrates that there are still several challenges concerning privacy, which solution is feasible to be extrapolated from highly-demanding environments like e-Health. Finally this paper reports our work mainly describing the basis of a privacy mechanism that uses an authorization paradigm based on a Mandatory Access Control model and, a novel architecture that propagates trust information based on a vehicle's geolocation.

***Keywords***: Authorization, privacy, security, trust management, VANETs**.**

## 1 Introduction

Vehicular Ad hoc NETworks (VANET) are a promising field of research and considering the extraordinary benefits expected from them, are one of the most relevant forms of mobile ad-hoc networks (MANET). Vehicular systems are an important problem of our society, where the common goal is to reduce road accidents; emerging technologies such as Dedicated Short-Range Communication (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 [1]), as long as all these messages are *trustworthy* they can greatly improve the overall road safety.

In the next years it is envisioned that 40% of all vehicular components will be electronic, with this integration vehicles will be equipped with communication and storing devices capable of storing and processing a great amount of information including driver's personal data and geolocation information. A VANET system can also be vulnerable to security attacks and must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission; another major concern is related with compromising the driver's privacy, being this, one of the main reasons to avoid the broad acceptance of this technology [2]. Thus privacy and trust issues of vehicular communications urgently need to be considered.

In privacy-conscious environments (i.e. 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. Our current research focuses on VANET's privacy and trust management from a driver's centric approach and it is based on two mechanisms:

- A Mandatory Access Control model inspired by eHealth systems, where the driver's explicit consent authorizes processing of his personal data.
- A novel architecture for trust propagation to acquire information about Certification Authorities and Attribute Authorities valid for a specific geographic area.

Such architecture is being prototyped over the Vehicular Information Transport Protocol VITP [3].

This paper is organized according to the following structure: Section 2 explains the main characteristics and applications of Vehicular Ad Hoc Networks. The fundamentals of trust and privacy in VANETs are described in Section 3. Section 4 surveys the related work. Section 5 introduces our proposed VANET's privacy model architecture and gives an overview of the suggested mechanisms. Finally in Section 6 we outline the main conclusions derived from this research and point out future work.

## 2 VANET's Components and Features

A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give drivers the time to react to life-endangering events [4]. A vehicle in a VANET is equipped with processing, recording and positioning features and is capable of running wireless security protocols [5] as shown in Figure 1.

In this section we overview VANETs' specific features and point out potential applications.

Received June 10, 2009

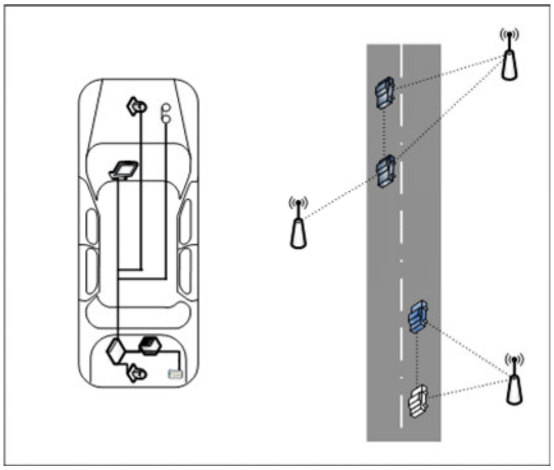

**Figure 1.** VANET's architecture

### 2.2 Features

Though vehicular ad hoc networks share general features with conventional ad hoc networks, VANETs have individual characteristics that are decisive in the design of the communication system [6], these include: *(i)* Dynamic topology, *(ii)* Mobility models, *(iii)* Infinite energy supply and *(iv)* Localization functionality.

### 2.3 Applications

VANETs enable vehicle-to-vehicle *(v2v)* and vehicle-to-infrastructure *(v2i)* communication, thus communicating nodes are either vehicles or base stations that can exchange information about traffic issues, road conditions and added value information. According to several authors: [4], [6], [7]) VANET's applications are commonly classified as follows:

- Warning: to prevent detected risky situations.
- Traffic management: to inform about traffic events.
- Added value: to provide numerous services (i.e. Internet).

## 3 Trust and Privacy in VANET's Environments

A comprehensive VANET security system should be able to help establishing the liability of drivers; but it should also protect the privacy of both, drivers and passengers [4], because of its importance to future deployments, this section will overview privacy and trust issues in VANETS.

### 3.1 Trust

The key element in a security system is *trust*: to be able to prevent any generic attack on vehicular networks, the system should use a secure and trusted communication infrastructure able to satisfy a set of security requirements ([4], [7], [8], [9]): *authentication*, *integrity*, *availability*, *non repudiation* and *privacy*.

In particular, for authentication purposes it has been proposed [4] for VANETs to use X.509 v3 digital certificates for entity's identification. For this authentication scheme it is required to validate and trust the Certification Authority (CA) that issued an entity's certificate. Both requirements pose a special challenge in VANETs, where multiple, unrelated CAs are likely to appear.

Trust issues are also important for authorization purposes, where the use of attributes certificates [10] is being considered: these credentials contain all information related with user's privilege attributes (information access rights) and are issued by an Attribute Authority (AA). Notice that in analogy to authentication issues, other authorization approaches (i.e. SAML) also require the use of digitally signed assertions and thus, trust checks involving one or more issuers.

### 3.2 Privacy Protection

Cars are highly personal devices that are kept for a long periods, therefore privacy of users should be enforced to protect its personal data from being disclosed to unauthorized observers. Innocent looking data from several sources can be collected over long periods and be automatically evaluated [11] to compromise privacy. Nowadays people are more concerned about their privacy, and for the successful deployment and public acceptance of VANET technology it is a significant factor: once privacy is lost, it is very difficult to re-establish that state of personal rights [11], [12] and the trust that people delivered into this technology. Even though from the drivers' point of view to achieve a perfect privacy is preferable, there exist different situations where being totally anonymous is not feasible: location privacy, for example should provide different levels of access to authorized entities (i.e. police).

In order to achieve the needed level of privacy and being able to provide the necessary security functionality, privacy threats should be determined just as presented next.

### 3.3 Privacy Threats

Vehicular communications should not become a weak link in terms of privacy, providing users at least with the same level of protection that is currently afforded without vehicular networks. 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 , *(iii)* vehicles cheating with information and *(iv) big brother* scenario where insurance companies may gather detailed statistics about movement patterns of cars.

The general principle in VANET's privacy is that information of 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). In the following section we give an overview of current research done about this topic.

## 4 State of the Art on VANET's privacy

Vehicular ad hoc networks have specially attracted a lot of attention in the academicals research community [13], as well as in the industrial domain mainly carried out by the Car to Car communication consortium [14], and many other projects like NoW [15], [16], PReVENT [17], and PATH [18] which cover several aspects from vehicular communication.

The importance of the security has been remarked in several studies ([2], [4], [7], [9]). In [2] the authors give a detailed analysis of general system attacks on Inter-vehicle Communication (IVC) and point out important system requirements concerning privacy. In [19] an extensive study and classification of trust models and its importance for ad-hoc networks are done. Authors of [20] proposed a solution for trust management in GRIDs; they mainly described important requirements towards establishing trust relationships in a GRID environment which according to the given scenarios behave in a very similar way to vehicular networks. In [21] different trust-establishment approaches are evaluated classifying them in various infrastructure-based and self-organizing mechanisms which according to VANET's characteristics are able or not to meet VANET's privacy requirements.

In past IVC projects, privacy issues have been a minor concern, however recently there has been increasing interest in trust and various related areas which are also relevant for us. In [11] potential implications of missing privacy are exposed and the author proposes to use centrally assigned digital pseudonyms, a downside could be the central authority which must not be within organizational control of a single manufacturer.

Authors of [22] define a system where vehicles change pseudonyms in certain region pointed by the system, this region should be where a lot of vehicles are within the communication range [11], a disadvantage could be when there are not enough vehicles changing pseudonyms within the region. To overcome this problem [23] proposes self assigned digital pseudonyms, taking a set of measures while changing pseudonyms:

*(i)* Synchronizing pseudonym change
*(ii)* Introducing gaps (silent periods)
*(iii)* Changing pseudonyms when nodes are in the region

This was also considered in [24] 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 [12], [25] proposes a silent period (random) in order to hamper linkability between pseudonyms and in [16] a study of practicability in pseudonymity deployment and implementation is done, where possible solutions are represented as a combination of existing pseudonymity algorithms concepts.

In [26] a security protocol based on group signatures is proposed by the authors, this protocol aims to guarantee security, anonymity and traceability (by authorized authorities). In [27] authors defined a protocol for conditional privacy preservation by proposing short-time anonymous key generation in order to minimize their number and ease their management. They also introduced a mechanism based on different levels of privacy consisting of a combination of levels of authentication, anonymity and unlinkability, which is a very interesting approach to cope with the privacy issues found by our research.

In summary, most of the research and proposed solutions in privacy mainly focus on the use of pseudonyms and algorithms for changing them. However for the application of pseudonymity into VANETs, open issues need to be solved [16]:

- It is necessary to identify the best opportunity to change a pseudonym
- Pseudonymity cannot prevent an attacker from collecting personal data
- Pseudonyms could be linked to the real identity in scenarios with a low number of participants
- User can link pseudonyms by an unchanged protocol in another layer
- Too frequent pseudonyms changes may affect routing feasibility.

Even though pseudonyms are important in VANET's overall security and are quite beneficial for protecting user's identity, neither full confidentiality nor access control to personal information are offered by these solutions. Pseudonyms could only be part of a privacy solution, but due to the overhead of their generation and storage the inclusion of them is not yet clear; therefore the need for more comprehensive mechanisms is still present.

Our research considers a privacy mechanism partially based on e-Health systems, which highly demand the protection of a patient's personal data. In our proposal, protecting a driver's personal information from being disclosed to unauthorized parties is given thanks to the use of a Mandatory Access Control model. The next section introduces this proposal.

## 5 VANET's Privacy Protocol

In this section we present the design principles of a VANET's privacy protocol that enables authorization decisions based on a Mandatory Access Control [28] and a geolocation-based mechanism for propagating trust between entities; the two main components of this architecture are introduced next.

### 5.1 Mandatory Access Control

The Mandatory Access Control model basically specifies who has what type of access to which targets and under which conditions. This model is inspired in e-Health and despite its simplicity; our research found that nowadays this environment enforces the most rigorous Data Protection laws (i.e. [29]) to enforce the privacy of patients and without sacrificing performance or usability.

In a Mandatory Access Control model, data confidentiality is provided by applying different authorization levels to an entity's personal information based on (i) the Simple Security Property (no read-up) and (ii) the *-Property (no write-down).

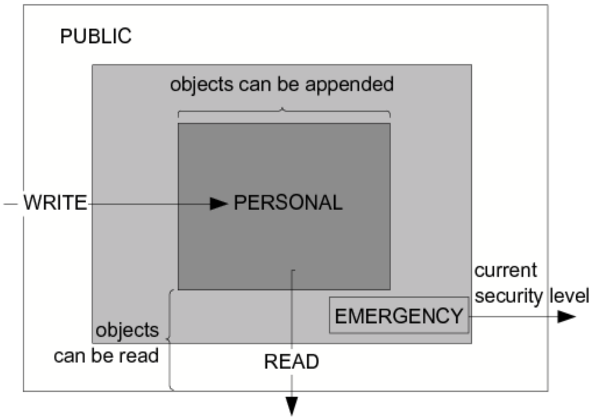

**Figure 2.** Relationship between authorization levels and access rights

In Figure 2 we show an example of applying this authorization model to VANETs, where the following levels of authorization have been defined:

- Personal: private information that should be disclosed only to previously authorized parties (i.e. authorized law enforcement agents); credentials of the entity are required.
- Emergency: information that should be disclosed in cases of emergency (i.e. paramedics if an accident occurred) credentials of the entity are required.
- Public: information accessible to any party, no authorization checks are required.

Through authorization levels it is possible to achieve different levels of privacy necessary to protect driver's personal information, which is not possible with the sole use of pseudonyms.

However, before an authorization decision can be taken for an entity willing to access a driver's data, it is mandatory to perform a trust evaluation on its credentials, that is, to authenticate and authorize it.

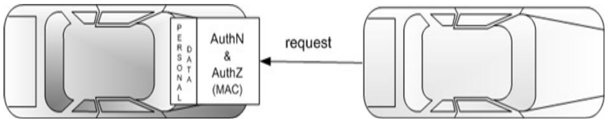

**Figure 3.** Vehicle to vehicle communication

In Figure 3 we show an example of a vehicle requesting personal information, let's assume this entity is an ambulance; given its security level "Emergency" and by applying this authorization model, the ambulance will be able to access only public and emergency information, and because its security level does not correspond to the security level defined by the personal data label, the access to personal information will be denied.

The authorization policy that will describe the defined entities and their role will be contained in the Tamper Proof device, signed by the Authorization Authority (possibly the CA), where the access will be granted if the security level of the requestor (`e_security_level`) is equal or higher than the security level denoted by the data's label (`data_label`) as shown in Table 1.

*Table 1.* Access control evaluation

```
Vehicle A (requestor):

/*Requesting information*/
request(data, my_security_level);

Vehicle B (responder):

/*Verifying data label*/
data label=getDataAccessLabel(requested_data);

/*Comparing data's access level with requestor's security level*/
if(e_security_level ≥ data_label)
  grant_access();
else
  deny_access();
```

However, comparing the security level of an entity with the information's label is not the only evaluation that should be performed by the system: an *entity trust evaluation* based on its credentials is necessary before assuming that any information received, specially the one concerning the security level, is authentic and because in general CAs and AAs are authoritative for a specific location (i.e. country), it is necessary for a vehicle to be aware of this information when moving around a VANET.

Because of the trust issues introduced in Section 3.1, our research has realized the need of a trust propagation system that communicates information about Certification Authorities and Attributes Authorities associated with a geographical area, just as explained next.

### 5.2 Trust Propagation Mechanism

In a Public Key Infrastructure [30], 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 these anchors will change with the vehicle's location, so this trust information needs to be propagated as soon as a driver joins a new geographical position, i.e. when traveling from Germany to France, once the driver crosses the border, new authority information should be sent as shown in Figure 4.

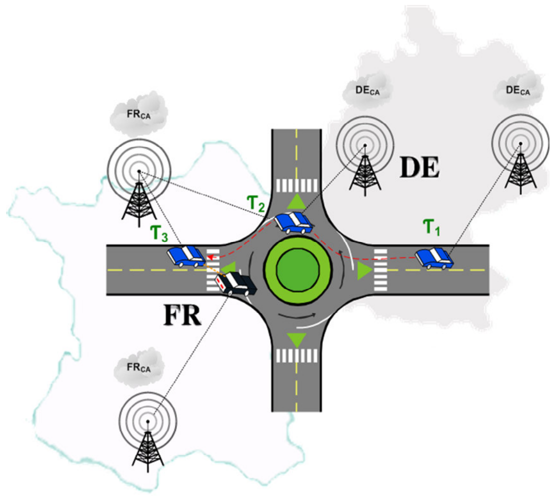

**Figure 4.** CA corresponding to a vehicle's geographical position

The data concerning CAs and AAs needs to be propagated on-the-road; therefore we believe that this mechanism may rely on protocols like VITP [3].

The proposed trust propagation mechanism uses a PKI infrastructure, and allows final users (vehicles into the VANET) to perform authentication in untrusted domains by dynamically enabling interoperability among different CAs without explicit agreements. To illustrate our proposal we introduced two use cases: the *vehicle to infrastructure communication (v2i)* and the *vehicle to vehicle communication (v2v)*, in both cases we proposed the use of a trusted third party able to authenticate digital certificates by providing access credentials that will be used for authorization purposes.

In the *v2i* scenario vehicles need to be able to access any authorized service available in the infrastructure, even in “untrusted” domains -those being serviced under a different Certification Authority-. The problems to address in this scenario are:

- How does the service authenticate the vehicle?
- How does the vehicle authenticate the service?
- To which service is the vehicle authorized to access?
- Which driver's information is the service authorized to access?
- What happens when the connections are lost?
- How to perform authentication and authorization when a vehicle moves between two different domains?

Similar to *v2i*, in the *v2v* scenario vehicles are able to request or offer information to other vehicles: for example a police vehicle requesting driver's information and current speed. The problems to solve in this scenario are:

- How do vehicles authenticate each other?
- Which information can be shared among vehicles?
- What happens when the communication is lost?
- How to perform authentication and authorization when vehicles belong to two different domains?

In current state of the art, authentication and authorization mechanisms for VANETs have been derived from traditional ones, however particular problems remain open *(i)* unreliable communications and brief connections require special care and (*ii)* cross certification agreements between untrusted domains are difficult to manage in VANETs. The mechanisms we propose are designed in order to take into account VANET requirements (i.e. unreliable and short communications) at design level; also our approach is performance-oriented and independent from the underlying technology and communication protocol. On the other hand, problems with cross-certification agreements due to the future deployment of VANETs will result in the creation of several PKIs, each one usually installing its own Certification Authority and thus giving birth to a large set of untrusted security domains that will represent a big interoperability problem.

To provide interoperability and cope with cross-certification issues, the proposed architecture implements the concept of *CA Federations*. 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 requirements are commonly a subset of the CA's Certificate Policy and can be audited at any time by the other members of the same Federation. When a new CA wants to participate in the Federation, it should pass through an “accreditation” process; once the accreditation has been passed the new member CA's root certificate is added to the trusted repository. Instead of distributing new sets of cross-certificates to all 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. This is a highly scalable approach for VANETs.

In the particular case of the example shown in Figure 4, the VANET Federation would include CA_$_{DE}$ and CA_$_{FR}$, therefore easing validation and trust issues. Worth to mention is that Federation models have proven quite useful in other multi-PKI environments, in particular the computational Grid [31].

A VANET can be modeled as a distributed system, where vehicles belonging to different domains must have certificates issued by different CAs. As shown in Figure 5 the architecture we propose includes an Interoperability System (IS) as an intermediary between certificate verifiers and the issuing CAs, by managing (retrieving, elaborating and updating) all information needed to create a dynamic CA Federation and allowing “on the fly” validation of Certificate Policies from unknown Certification Authorities.

The IS must perform two main tasks: *(i)* online validation of the certificate's status and *(ii)* evaluation of the issuing CA's security level. To achieve these functionalities, the IS's is based in two components: a *Certificate Validator* which uses a high level OCSP responder to provide near-real time status information of certificates issued by any member of the CA Federation (in analogy to the system presented in [32]), and a *Trust Evaluator* which consists of a PKI evaluation system for computing a CA's security level. For the latter, a mechanism like the Reference Evaluation Model (REM) can be adopted, just as shown in [33]. The quantitative CA's security level obtained through REM can be used afterwards to enforce privacy by performing authorization decisions based on the MAC (Section 5.1).

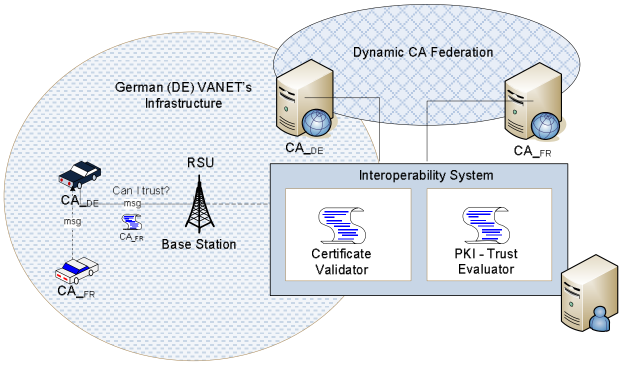

**Figure 5.** Trust Management Architecture for VANETs

In Figure 5 and Figure 6 we depict the trust propagation framework and the communication flow between the vehicles and the different components of this architecture, taking into account the example given previously in Figure 4: when a vehicle travels around Europe, let's say a French vehicle traveling to Germany, and tries to communicate to local German vehicles -which of course belong to a different trust domain, the German vehicle receives a message but does not know whether or not to trust this message.

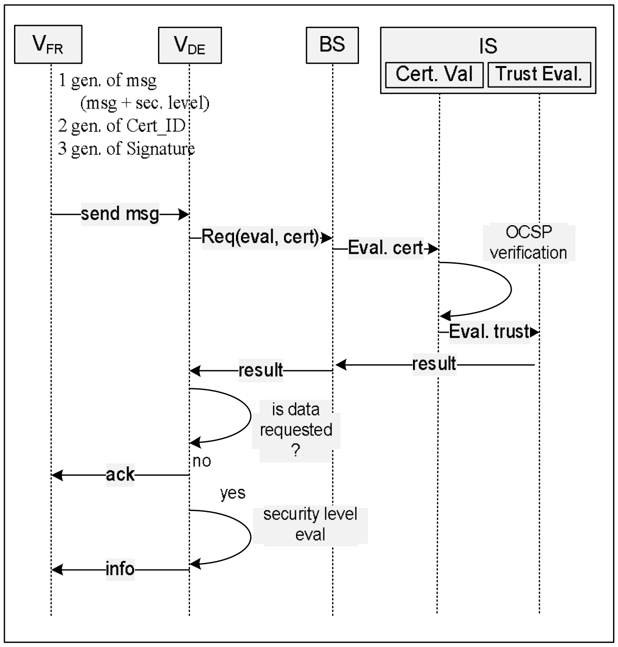

**Figure 6.** Messages required by the Trust Propagation mechanism

In order to verify the French vehicle's message the German one communicates to the infrastructure via a base station, allowing the IS to validate and evaluate the sender's certificate and to take the decision if it is possible or not to trust in the certificate issuer (CA_FR), once the German vehicle gets the response from the base station, depending on the message's content and purpose a corresponding action should be done. In this example we have considered two possible situations:

- A warning message was received: then vehicle sends an acknowledgement and forwards the received message,
- Information was requested: then the requestor's security level should be evaluated, just as shown in Figure 6.

In addition to achieving conditional trust and privacy requirements, designing the proposed security architecture took into consideration other issues such as performance, by means of packet overhead, packet sending rate, and requirements on packet loss rate and message latency. To achieve these features, we have considered the message structure shown in Table 2, which takes into account performance requirements but without compromising security and privacy in the overall architecture.

*Table 2.* Warning message

| Packet format | |
|---|---|
| Payload = Message + Cert_ID | Signature |
| 110 bytes | 110 bytes |

Table 2 has considered 110 bytes of payload for a typical warning message which includes the `Cert_ID` based on the originator's ID, which basically consists of a code generated considering the transformation from Equation 1. The second part is also approximately 110 bytes and corresponds to the message's signature[1].

$$E_{Kpub_{IS}} = \left\langle ID\_user\_cert \,\middle|\, random(timestamp, nonce) \right\rangle \qquad (1)$$

Where:

- $E_{Kpub\_IS}$ is the encryption with the public key of the Interoperability System, stored in the vehicle's tamper proof device to avoid compromise.
- *ID_user_cert* is the Subject's Distinguish Name of the sender's X.509 certificate.
- *random(timestamp,nonce)* is provided as a defense against re-play attacks.

Thanks to this transformation it is possible to preserve the confidentiality of the sender, in such a way that only the IS will be able to identify the message's sender in case needed, providing privacy via confidentiality.

[1] Using a RSA signature with a 1024 bits private key.

According to [1], if we suppose the use of DSRC (Dedicated Short-Range Communications) as the standard communication channel for VANETs and considering the maximum data rate of 6 Mb/s -where messages are sent every 300 ms-, then it is possible to maximize bandwidth usage and reduce processing overhead. Taking into account the previous information, we have tried not to add excessive overhead to these packets, assuming a final size for a warning message of 220 bytes, which is feasible due to the characteristics of the overall system.

## 6 Conclusions and Future Work

VANET's privacy and trust have been identified to be profoundly important; on one side users need to trust that their personal information will be protected against misuse or unauthorized access, and on the other side authorities should be able to identify misbehaving units. This paper presented existing privacy and trust issues, finding that so far these approaches consider that privacy mostly rely on the use of pseudonyms. However, pseudonymity does not offer any authorization scheme and cannot prevent the unauthorized collection of data; therefore these solutions for privacy matters are not enough.

We proposed the use of a privacy solution based on two mechanisms: a Mandatory Access Control and a novel Geolocation-based Trust Propagation. The former is inspired in e-Health systems which define access levels for accessing different parts of personal data. The latter mechanism is used to obtain trust information concerning Certification and Attribute Authorities valid for a specific location.

As a future activity this research work plans to contribute with a privacy-aware VITP protocol implementing the geolocation-based trust propagation. We plan to define the policies, their security aspects and to develop a mechanism to evaluate the CA's and VANET's nodes trust level, also taking into account a scenario when there is no available infrastructure.

To cope with performance and security issues, we will consider testing different algorithms in order to minimize the security information carried by the packet, as well as the consideration and design of other type of messages exchanged by the system (i.e. verification messages). By performing simulations we expect to measure, for example, the necessary number of messages and latency required to propagate trust information in complex CA hierarchies

## Acknowledgment

This article is an extended version of the paper "Geolocation-based Trust for Vanet's Privacy" published in the Proceedings of the Fourth International Symposium on Information Assurance and Security (IAS 2008) held at Naples, Italy. We want to thank the anonymous reviewers and the organizers of the conference, especially Dr. Ajith Abraham. Finally, this work is financially supported by INTEGRA (CENIT-Integra, C-07588).

## References

[1] U.S Department of Transportation: "National Highway Traffic Safety Administration". *Vehicle Safety Communications Project, Final Report.* USA, 2006.

[2] A. Aijaz, B. Bochow, F. Doetzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmller. "Attacks on inter-vehicle communication systems - an analysis". In *WIT '06*, (Hamburg, Germany), 2006.

[3] M. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," *Selected Areas in Communications, IEEE Journal on,* vol. 25, no. 8, pp. 1590–1602, Oct. 2007.

[4] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *SASN '05*, (New York, NY, USA), pp. 11–21, ACM, 2005.

[5] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," Security and Privacy, IEEE, vol. 02, no. 3, pp. 49–55, May-June 2004.

[6] A. Zanella and E. Fasolo, "Inter-vehicular communication networks: a survey," in *2nd Internal NEWCOM Workshop*, 2006.

[7] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *ARES'06*, p. 8, 20-22 April 2006.

[8] S. Eichler, F. Dotzer, C. Schwingenschlogl, F. Caro, and J. Eberspaher, "Secure routing in a vehicular ad-hoc network," in *VTC '04*, vol. 5, pp. 3339–3343 Vol. 5, 26-29 Sept. 2004.

[9] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for vanets," in *ESCAR '06*, (Berlin, Germany), 2006.

[10] D. W. Chadwick and A. Otenko, "The permis x.509 role based privilege management infrastructure," in *SACMAT '02*, (New York, NY, USA), pp. 135–140, ACM, 2002.

[11] F. Doetzer, "Privacy issues in vehicular ad hoc networks," in *Privacy Enhancing Technologies*, Lecture Notes in Computer Science pp. 197–209, Springer 2005.

[12] M. Gerlach, "Trust for vehicular applications," *ISADS'07*, pp. 295–304, 21-23 March 2007.

[13] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," Tech. Rep. IC/2004/24, Federal Institute of Technology Lausanne, School of Computer and Communication Science, 2004.

[14] "Car to Car Communication Consortium (C2CCC)." http://www.car-to-car.org/, 2009.

[15] "Network on Wheels (NoW)." http://www.network-on-wheels.de/, 2009.

[16] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in vanets - putting pseudonymity into practice," *WCNC '07*, (Hong Kong, China) pp. 3400–3405, 11-15, March 2007.

[17] "Prevent project." http://www.prevent-ip.org/, 2009.

[18] "California Partners for Advanced Transit and Highways (PATH)." http://www.path.berkeley.edu/, 2009

[19] S. Chinni, J. Thomas, G. Ghinea, and Z. Shen, "Trust model for certificate revocation in ad hoc networks," Ad Hoc Netw., vol. 6, no. 3, pp. 441–457, 2008.

[20] E. Papalilo and B. Freisleben, “Managing Behaviour Trust in Grid Computing”, *Journal of Information Assurance and Security (2008),* vol. 3, no. 1, pp. 27-37, March 2008

[21] A. R. Beresford and F. Stajano, “Mix zones: User privacy in location-aware services,” in *PERCOMW '04*, (Washington, DC, USA), p. 127, IEEE Computer Society, 2004.

[22] P. Wex, J. Breuer, A. Held, T. Leinm¨uller, and L. Delgrossi, “Trust issues for vehicular ad hoc networks,” in *VTC* Spring, pp. 2800–2804, IEEE, 2008.

[23] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in vanets,” in *VANET '04*, (New York, NY, USA), pp. 29–37, ACM, 2004.

[24] M. Gerlach, “Assessing and improving privacy in vanets,” in *ESCAR '06*, (Berlin, Germany), 2006.

[25] K. Sampigethaya, L. Huangy, M. Li, R. Poovendran, K. Matsuuray, and K. Sezaki, “Caravan: Providing location privacy for vanet,” in *ESCAR '05*, 2005.

[26] P. H. H. X. Lin, X. Sun and X. Shen, “Gsis: A secure and privacy preserving protocol for vehicular communications,” in *IEEE Transactions on Vehicular Technology*, pp. 3442–3456, 2007

[27] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *INFOCOM*, pp. 1229–1237, IEEE, 2008.

[28] D. E. Bell, “Looking back at the bell-la padula model,” in *ACSAC '05*, (Washington, DC, USA), pp. 337–351, IEEE Computer Society, 2005.

[29] “Sealed Envelopes” Briefing Paper: “Selective Alerting Approach,” tech. rep., Connecting for Health, National Health Service, 2006.

[30] R. Housley, W. Polk, W. Ford, and D. Solo, “Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.” RFC 3280 (Informational), 2002

[31] “International grid trust federation.” http://www.gridpma.org, 2007.

[32] J. Luna, M. Medina, and O. Manso, “Using ogro and certiver to improve ocsp validation for grids,” in GPC (Y.-C. Chung and J. E. Moreira, eds.), vol. 3947 of Lecture Notes in Computer Science, pp. 12–21, Springer, 2006.

[33] V. Casola, J. Luna, O. Manso, N. Mazzocca, M. Medina, and M. Rak, “Interoperable grid pkis among untrusted domains: An architectural proposal,” in GPC (C. C´erin and K.-C. Li, eds.), vol. 4459 of Lecture Notes in Computer Science, pp. 39–51, Springer 2007.

## Author Biographies

**Jetzabel Serna** Was born in Aguascalientes (Mexico) in 1980. She obtained her Bachelor’s degree in computer systems engineering from the Technical Institute of Tijuana (Tijuana, Mexico) in 2001. She achieved a Master of Sciences degree in computer science and communications engineering from the Gerhard Mercator University (Duisburg, Germany) in 2006. Since 2006 doing her PhD at the Technical University of Catalonia in the Computer Architecture Department (Barcelona, Spain), and working as a research assistant in the Network Security Group. Her topics of interest are security, trust and privacy in mobile environments.

**Jesus Luna** Was born in Mexico City (Mexico) in 1972. He obtained his Engineering diploma in telecommunications and electronics from the "National Technical Institute" (Mexico City, Mexico) in 1995. He achieved his M.Sc. degree in computer sciences from the "Technical Institute of Higher Studies of Monterrey" (Mexico City, Mexico) in 2003. Finally he obtained his PhD degree in computer architecture from the "Technical University of Catalonia" (Barcelona, Spain), where he graduated with honors in 2008. Currently works as Senior Security Researcher in "Barcelona Digital - Centre Tecnològic" and his topics of interest are Grid/Cloud security, trust and security for emerging technologies (Vehicular Ad-hoc Networks and Wireless Sensor Networks) and applied cryptography.

**Manel Medina** Was born in Barcelona (Spain) in 1952. He obtained his Engineering diploma in telecommunications from the Technical University of Madrid - UPM (Madrid, Spain), received his PhD in telecommunications from the Technical University of Catalonia (Barcelona, Spain) in 1981. He is Full Professor at the Technical University of Catalonia (UPC) since 1992. He is Chief Innovation Officer of SeMarket and Security Projects Officer of Barcelona Digital Technological Center. Head of esCERT-UPC, Spanish Computer Emergency Response Team and of the Internet Applications research center (UPC). Head of cANet, research center of Internet Applications of the UPC and full Member of ESRIF (European Security Research and Innovative Forum) (since 2006) to advise European Commission about security research topics in the R&D funding programs.