This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

Security models in Vehicular ad-hoc networks: a survey

J. M. de Fuentes, L. Gonzalez-Manzano, A.I. Gonzalez-Tablas and J. Blasco

Abstract— **The security and privacy issues of vehicular ad-hoc networks (VANETs) must be addressed before they are implemented. For this purpose, several academic and industrial proposals have been developed. Given that several of them are intended to co-exist, it is necessary that they consider compatible security models. This paper presents a survey on the underlying security models of 41 recent proposals. Four key aspects in VANET security are studied, namely trust on vehicles, trust on infrastructure entities, existence of trusted third parties and attacker features. Based on the survey analysis, a basic mechanism to compare VANET security models is also proposed, thus highlighting their similarities and differences.**

***Index Terms*—Vehicular ad-hoc networks (VANETs), security model, trust.**

I. Introduction

Vehicular ad-hoc networks (VANETs) are a new communication scenario in which vehicles can exchange information. VANETs are one of the enabling technologies of Intelligent Transportation Systems (ITSs).

One of the main aspects of ITSs is that security and privacy issues must be addressed before their implementation. For this purpose, in recent times several academic and industrial proposals have been developed. They cover the main security requirements, namely anonymity/privacy, data integrity, sender authentication, data trust and availability. On the other hand, different standards that address these issues have been approved. Among them, IEEE 1609.2 [42] and ISO 21217 [43] are the most representative ones.

Several ITS services may be offered at the same time to each vehicle. To achieve this goal, it is necessary that these services are based on compatible security models, i.e. a common set of assumptions that enable them to be coexistent. For example, if a service requires the vehicle to be identified with a permanent identifier, whereas another one imposes that the vehicle has only a set of pseudonyms, it is not possible to have both services at the same time. The situation gets worse when standards are taken into account. Usually assumptions are made without considering these norms and potentially creating a conflict with their terms.

Taking into account the previous facts, it is necessary to establish a clear view on the assumptions that are made, in order to verify the compatibility of different proposals. The goal of this work is to perform a survey on the assumptions that form the underlying security model of different proposals. The survey is performed over a sample of 41 contributions from the last six years, thus presenting an overview of recent works. This survey focuses on key aspects of these models, namely trust on vehicles and infrastructure nodes, existence of trusted third parties and attacker features. Based on the survey results, a simple mechanism to compare models is proposed, thereby highlighting their similarities and differences. This is a first step towards an in-depth compatibility evaluation of these models.

Paper organization. Section II gives a background on vehicular ad-hoc networks and their related security issues. Section III provides an overview of the survey and its scope. Section IV presents the results of the survey performed over a sample of 41 papers. Section V describes the related security issues as defined in representative standards. Section VI discusses the results obtained from the survey and compares them to the mandates of standards. Section VII presents the basic approach to compare proposals based on their security models. Finally, Section VIII describes the related work and Section IX concludes the paper.

II. Background. Vehicular ad-hoc networks and security needs

In this Section, a brief overview of the main elements appearing on Vehicular ad-hoc networks (VANETs) is given, along with the security-related needs usually considered in these networks.

A. Basic scheme

Several entities are usually assumed in VANETs (Figure 1). Typically, one or more vehicles are connected to one or more static nodes (called Road-Side Units, RSUs) in order to

Authors are with the Computer Science Department of University Carlos III of Madrid, Spain. Avda Universidad, 30, 28911 Leganes (Spain).

e-mail: {jfuentes, lgmanzan, aigonzal, jbalis} @ inf.uc3m.es.

Corresponding author: J. M. de Fuentes, phone:0034916245957.

This work is partially founded by Ministerio de Ciencia e Innovacion of Spain under grant TIN2009-13461 (project E-SAVE).

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

exchange information with them or with a set of infrastructure nodes. Given the nature of these entities, two different contexts may be identified, namely the infrastructure context (in which RSUs connect to infrastructure nodes) and the ad-hoc one (where vehicles and RSUs are connected).

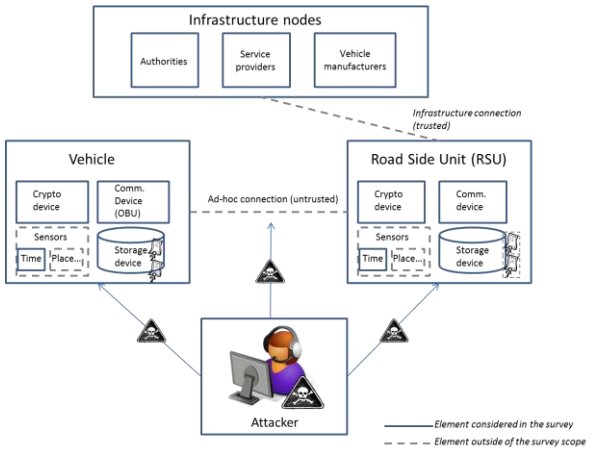

Fig. 1. Overview of a vehicular network. Elements covered in this survey are highlighted

Those entities managing the traffic or offering an external service are placed in the infrastructure context. Thus, the legal authority, the set of service providers and even vehicle manufacturers belong to this environment. Depending on their trustworthiness they may be considered as Trusted Third Parties (TTPs), that is, entities that are fully reliable for their context of operation.

In the ad-hoc environment, sporadic communications take place to and from vehicles. For this purpose, vehicles are equipped with a communications unit (called OBU, On-Board Unit). They also have a set of in-vehicle sensors that enable them to measure their immediate environment and their own status. In order to process this information, computational devices and storage units are also assumed to be present in vehicles.

B. *Security and privacy needs*

VANETs, as any other communication network, require a set of security and privacy needs to be fulfilled in order to ensure a successful use and public acceptance [48], [49].

One key aspect in these networks is the existing trade-off between liability and privacy. Thus, it is necessary not only to uniquely *identify* each communicating node, but also to *authenticate* it. In this way, it is possible to determine the liability for a malicious action (e.g. vehicles sending bogus information). A related security need is *non-repudiation*, which ensures that an entity performing an action will not be able to deny having done it.

Nevertheless, *privacy preservation* is critical in these networks. It must be impossible for an unauthorized party to trace the path followed by a given vehicle. This need is present in all location-based services [52]. What is particular of VANETs is that the attacker must not be able to link a vehicle's identity with that of its driver/owner. This guarantee must remain unless a malicious action is committed.

Related to information security, there are three main needs. First, *confidentiality* (i.e. ensuring that messages will only be accessed by the intended parties) is required in some private services, like location-based ones. Secondly, *data integrity* ensures that they have not been altered since their creation. Even beyond, the third need is related to guaranteeing *data trust*, i.e. data are fresh, updated and reliable.

The last need is *availability*, which implies that every node must be able to timely process and send the required information. Nevertheless, this is a general requirement as its fulfillment depends on the resource-saving design of the mechanisms that provide the remaining services.

III. Survey Overview and Scope

The survey presented in this paper covers the different VANET elements over which assumptions are commonly made (Figure 1). Particularly, the security of the main VANET entities (namely vehicles, RSUs, infrastructure nodes and attackers) will be considered. A general view on the survey contents is presented in Figure 2. The choice of the aspects to be studied comes from an in-depth analysis of the selected works. The aim is to choose those issues that are usually subject to different assumptions, thus leading to diverse (even contradictory) scenarios.

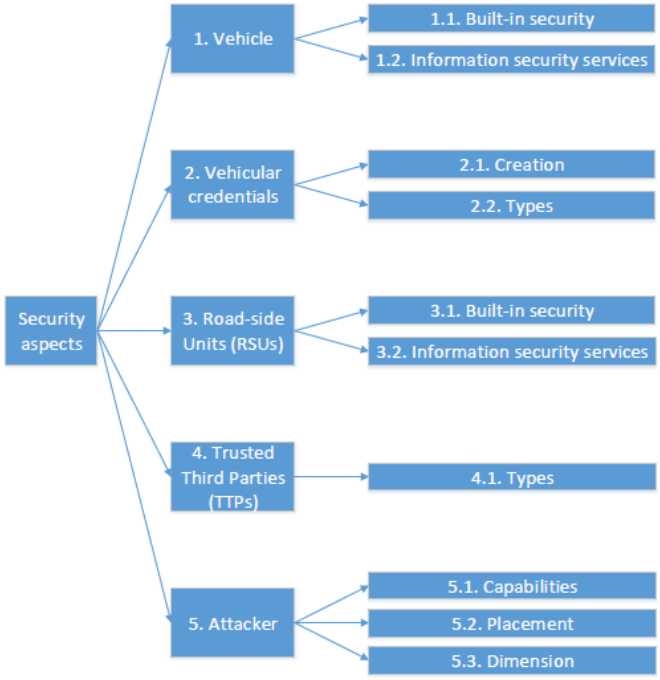

Fig. 2. Survey contents overview

For both vehicles and RSUs, the built-in trust of their internal devices will be analyzed. Whereas some proposals

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

assume that they are untrusted, others suppose that they have different degrees of tamper protection. Furthermore, on top of this trust some interesting security properties (e.g. secure storage) may be offered. Their existence is analyzed as well.

Due to the needs of authentication, privacy and confidentiality in this environment, the different types of vehicular credentials are also surveyed. A broad overview on the plethora of cryptographic approaches that are being proposed in this context is given. Furthermore, one controversial aspect that is also surveyed is their management process and particularly their creation. From classical, centralized approaches to fully decentralized ones, different settings are studied.

Concerning infrastructure entities, it will be analyzed which of them are considered as trusted. In such a case, they are commonly referred to as Trusted Third Parties (TTPs). The focus is on their nature, as some works assume that they are related with the Government while others base on their independence. Furthermore, other transportation-related stakeholders (like service providers) are considered TTPs in some proposals.

Regarding the attacker, three key aspects are covered – what it can do (e.g. inject packets), where it is placed (e.g. in vehicles) and which is its dimension (e.g. if honest majority is assumed).

A. Limitations

Three security-related aspects are left out of the scope of this survey. First, credentials of RSUs are not reviewed herein, as this matter is less challenging from the research point of view. There are two reasons behind this decision. On the one hand, RSUs have higher computational resources than vehicles, which enable them to use a wider amount of cryptographic primitives. On the other hand, RSUs are assumed to be supervised by the road traffic authority, thus enabling an easier credential management procedure.

Secondly, sensor trust is not addressed, as they have low reliability in vehicles (see [50]) and they are not so relevant in RSUs. The only exception is on the time source, which may be seen as a specific type of sensor. Having reliable time information is a premise for the development of some security-related mechanisms, so it is worth studying.

Last but not least, connections between RSUs and infrastructure nodes or vehicles (recall Figure 1) are not addressed since their security profile is usually the same. Thus, connection with infrastructure is frequently considered reliable, as it may be protected with well-known mechanisms taken from regular communication networks. In practice, it means that it is a confidential, authenticated channel in which data integrity is preserved (e.g. [5], [9]). On the other hand, connection with vehicles is usually unreliable and untrusted – data may get lost or even maliciously modified.

IV. Review on Security Models

In this Section, a revision of the security models considered in VANET-related recent works is presented. Section IV-A addresses the security of the vehicular devices and credentials (Figure 1, left part), whereas Section IV-B focuses on that of road-side units (Figure 1, right part). Section IV-C introduces the assumptions on a particular set of infrastructure nodes (Figure 1, upper part), called Trusted Third Parties (TTPs), which are relevant for the security matters. Finally, Section IV-D describes the nature and capabilities of considered attackers (Figure 1, lower part).

For the sake of clarity, each of the following Sections have an accompanying Table in which a detailed view of each issue is presented for all considered works. These Tables are organized following the structure presented in Figure 2. Particularly, columns are separated according to that structure whereas each row describes one considered proposal. To improve the work readability, all tables have been placed in the Appendix.

A. Analysis on vehicle-related assumptions

This Section focuses on the assumptions made over vehicular devices and credentials. With respect to devices, the analysis on their trust will address both its physical (built-in) protection as well as the offered security services. These issues are summarized in Table I. With respect to credentials, both their creation and their type will be studied. Table II summarizes these issues for the works at stake.

1) Trust: One of the most significant aspects of the survey is that most contributions (22 out of 41 proposals) do not detail the required trustworthiness on the vehicular side. It must be noted that the reviewed works are focused on providing security services over vehicular networks. For this purpose, they make use of cryptographic operations and they manage private data. Therefore, having an explicit degree of trust in the vehicular side seems to be mandatory in all proposals. Despite this fact, the proposal in [7] states that the vehicle may be completely untrusted. Nevertheless, according to their description this statement is not accurate, as at least the storage of credentials must be protected against illegal access.

Among the proposals that describe this trust, most of them (11 out of 19) assume that reliable storage is provided. A lower amount (9 out of 19) rely on the assumption about reliable cryptographic processing, whereas only a small fraction (5 out of 19) consider that there is a reliable time source.

The previous figures also contain those proposals in which it is stated that vehicular devices are *fully trusted*. In these cases, it has been assumed that there is a Trusted Platform Module (TPM). According to [47], this device provides with secure storage, cryptographic computation and an internal reliable clock.

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

Apart from the general features of these devices, the extent of physical protection against tampering has also been analyzed. Particularly, there are some contributions (8 out of 19) which are based on tamper-resistant hardware, that is, a component which is able to actively react to a physical manipulation. Smart cards (used in [27]) and TPMs are examples of this family of devices. On the other hand, a smaller amount (6 proposals out of 19) consider tamper-proof device, which only gives evidence on such a malicious alteration.

Despite the existence of the aforementioned devices, in [11] it is stated that cryptographic operations are not carried out by this device. Instead, a processing unit (not explicitly trusted) performs them. In a similar way, [41] performs decryption and a generation of a cryptographic policy tree in the On-Board Unit (OBU). It must be noted that in the aforementioned paper, trust assumptions are made over the tamper-proof device, but not over the OBU.

One important point is that none of the revised approaches makes assumptions on the trustworthiness of the internal communication networks. Thus, despite the assumption of having secure storage, in absence of a trusted internal network it could happen that maliciously forged information is securely stored.

2) Credentials: Vehicular credentials enable the electronic identification and authentication of the vehicle within the network and the provided services. As a difference with vehicular trust assumptions, only two proposals ([3], [38]) do not include any consideration on this issue. The remaining ones have specified the required type of credential. Nevertheless, a category has been included to classify future works that do not make use of credentials (e.g. reasoning mechanisms over sensorial data).

One important difference between all proposals is the procedure to create these cryptographic materials. A significant amount of them (18 works) propose a combined approach in which vehicles or RSUs are enabled by the authority to perform this operation. Afterwards, this material is certified by the authority. The other two alternatives are a fully centralized approach in which a trusted authority generates these materials (13 proposals) and a fully distributed architecture, in which vehicles create them (7 proposals).

Concerning identification, 17 proposals make use of a single identifier which remains unchanged over time. As this identifier could enable following the path of the affected vehicle (tracking), an alternative taken by 4 works is the use of pseudonyms. Other group of 4 proposals use attributes to identify the vehicle, either permanent ones (e.g. make, model) or temporary ones such as its localization. The use of a public value as identifier (which is the base of Identity-based cryptography) is present in 2 proposals.

With respect to the authentication, the most noteworthy assumption (26 articles) is the use of public key cryptography – there is a pair of public-private keys, being the public key associated to the corresponding certificate. In fact, the most common choice among them (16 out of 26 proposals) is the creation of a pool of pseudonym-based, short-lived certificates. The rest of works based on public key cryptography either avoid the use of certificates (8 articles) or use anonymous certificates (3 proposals). It must be noted that the aforementioned use of identity-based cryptography is opposed to the public key one, as there are no explicit certificate management procedures.

Among the remaining authentication mechanisms, 5 proposals make use of a group key. The same amount considers that the vehicle stores a private, unique key. Also, 5 works are based on the use of a session key.

B. Analysis on RSU-related assumptions

Even if a significant amount of the analyzed contributions (13 articles) do not assume that RSUs are in place, most of the surveyed works make an active use of this element. This Section introduces the assumptions on trust related to RSUs. Table III summarizes the different issues considered for each paper.

As it happened with vehicular devices, RSUs usually perform cryptographic operations in the considered proposals. Despite their implication on the proposed approaches, it is noteworthy that a significant amount of works (14 out of 41) do not detail the trustworthiness of RSUs. This set of articles is formed by those that mention the existence of RSUs but do not give any detail on their implication and trust. Besides, 4 works assume that RSUs are untrusted.

With respect to the remaining contributions, a small fraction of them (6 articles) consider RSUs to be fully trusted. As it happened with vehicles, this issue has been reflected as if they were equipped with a tamper-resistant hardware that provides with secure storage, processing and time information. Taking into account this decision, each feature is considered independently in different proposals – 9 assume that RSUs perform reliable cryptographic processing, the same amount consider reliable storage and a smaller amount (6 works) suppose the existence of a trusted time source.

From the physical point of view, apart from tamper-resistant hardware, 3 works consider that RSUs are equipped with a tamper-proof device. In order to reduce the trust level, in [7] RSUs are semi-trusted in that they operate as expected but they can leak data.

C. Analysis on TTP-related assumptions

Except from 5 proposals, most revised ones assume the existence of different trusted third parties (TTPs). The most common party is a Certification Authority (CA) assumed in 23 works (see Table IV). Apart from the centralized, fully trusted CAs, there are other variants – it may be distributed among different entities (e.g. [35]) or it may be semi-trusted [31]. Other two usual entities are a generic trusted authority which

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

appears in 12 contributions and a government-related authority that is assumed in 6 articles.

The proposals that make use of the concept of group of vehicles usually assume that there is an entity different from the CA that manages the group. This entity is usually referred to as Group Manager and appears in 3 contributions. This role may be spread in two different entities, called Membership Manager and Tracing Manager, to share responsibility and reduce the chance of performing malicious actions [20].

In some cases, the revised approaches also rely on the existence of two real-world entities related to the vehicular context – vehicle manufacturers ([34]) and service providers ([26]), being these providers in charge of offering an ITS-related service. It must be noted that these entities are usually not fully trusted, but they act as such in the proposed approaches.

D. *Analysis on attacker-related assumptions*

The type of attacker considered in a given security model is a significant aspect, since it points out the degree of threat that must be countered. Therefore, it is necessary to clarify which malicious actions can be performed. Furthermore, it must be stated the scope of the attacker. This scope is determined by the attacker's nature (i.e. if it is placed in one or more vehicles/RSUs) and dimension (i.e. whether it acts independently or may collude, its degree of presence and coverage). Both the attacker capabilities and its scope are introduced below.

1) *Attacker capabilities.* Seven main threats against the security needs presented in Section II-B have been identified. They are related to the information security (eavesdropping, modification, injection), to the entities' privacy (tracking, impersonation), to the availability (jam) or to the physical integrity (OBU hacking). Each of these threats is shown in a column of Table V, under the "Capabilities" heading. Given that in order to perform tracking it is necessary to eavesdrop, both issues are presented in the same column in that table.

The most common capability is to perform eavesdropping and impersonation, both appearing in 21 proposals. It seems reasonable since these actions may lead to risks that are especially relevant in the vehicular context – tracking vehicles and creating the illusion of a group of vehicles from a single one.

A lower but significant amount of works (18 proposals), consider that the attacker may inject or replay packets in the communications network. On the other hand, a similar amount (15 proposals) assume that it may forge or erase information. These results illustrate that a significant portion of the research community is aware of the existing risks in the vehicular communication channel. It must be recalled that this is a wireless, shared medium in which any nearby entity can have access. However, paper [3] assumes that injection cannot be performed by the attacker.

The threats of jamming and physical hacking of the vehicular devices are only present in a small fraction of works – 6 and 4 articles, respectively. Furthermore, the proposal in [35] assumes that both threats cannot be performed. The low amount of contributions addressing these issues may be due to two main reasons. First, both threats do not affect to a single piece of information or entity, but to all of them. They affect to the global chance of communication. The second reason, which applies particularly to jamming, is that it may be alleviated through a suitable design of the remaining security mechanisms that involve communication.

Taking into account these issues, most surveyed proposals assume that these threats have already been addressed instead of particularly countering them. This is usually done by citing a previous work that faces this issue. As an example, paper [18] which tackles these threats has been already cited more than 140 times according to Google Scholar.

2) Attacker scope: nature and dimension. The scope of the attacker is only stated in a discrete amount of the surveyed works (17 out of 41). Concerning its nature, 6 proposals assume that it is placed in vehicles whereas only 2 consider that it acts in RSUs.

The amount of attackers and how they interact is given by its dimension properties. In this study, three issues have been considered. First, 8 papers state that there are several adversaries and that they can collude, whereas the proposal in [34] assumes no collusion. The second factor is the density of adversaries, being the assumption of honest majority present in 6 articles. The last factor is the attacker coverage, in which 4 contributions assume that it may have global coverage. It must be noted that in these works it would be reasonable to have a lack of indications on the attacker nature -- it should be deployed over the whole network in order to have a global action range. However, the works in [7] and [13] specify that it is placed in vehicles.

V. STANDARDS POSITION ON SECURITY MODELS

There are two sets of standard families that are relevant to the security field. On the one hand, CALM (Communication Access for Land Mobiles) standards are being defined by ISO. Among them, ISO 21217 defines the general architecture including the security issues [43]. Within this norm, two security-related documents[1], namely ISO 11776 and ISO 11769 are cited. These are technical reports that cover the security considerations for lawful interception and data retention [44], [45]. These issues are required to support the work of enforcement agencies. Particularly, they define how interception must be performed and for how long data must be retained. These requirements are related to how the service provider may operate, but they do not make assumptions or statements over vehicular devices, RSUs, TTPs or attackers.

A similar situation happens with the technical report ISO

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

12859 (not mentioned in [43]), which covers privacy in intelligent transportation systems. Besides the fact that ISO's technical reports are informative (i.e. not normative), this document only contains recommendations over the elements considered in this work. As an example, this document states that special attention must be put on the storage, transmission and processing of information, providing the required access control. In sum, this is a design goal and not a decision that defines the security of each element at stake.

The second family of standards is the WAVE (Wireless Access in Vehicular Environments) one developed by IEEE. Among them, IEEE 1609.2 is the one focused on security issues [42]. IEEE 1609.0 will describe the general architecture, but it is still under development.

Considering the previous facts, the two references that have strong relationship with security models are ISO 21217 and IEEE 1609.2. Each one will be introduced in the following subsections.

A. *ISO 21217*

ISO 21217 describes the common architectural framework of CALM-compliant ITS stations. These stations may be located at vehicles, RSUs, centralized entities or personal devices such as cell phones.

In general words, each station may be divided into one or more internal components. This standard determines that there is a security module inside each of these components. This module manages three elements – first, the firewall and intrusion detection system; second, the authentication, authorization and profile management module; and third, the identity, certificates and cryptographic material. It also contains the functionality provided by a Hardware Security Module (HSM), although the capabilities offered by this device are not clarified.

Despite the existence of such a component, the current version of this standard does not contain its specification. These details will be added in a future revision, as the development of security functionality is under consideration by ISO/TC 204 (WG 16). Nevertheless, according to the current text and the use of HSMs it is possible to devise that this standard will state that all ITS stations need to provide with reliable storage (at least of the material cited in the previous paragraph) and reliable cryptographic processing. The type of built-in security (e.g. tamper-proof, tamper-resistance) is not clear according to the current document wording. It should be noted that the existence of these internal security components does not imply any kind of particular implementation -- they may be implemented in a single device or split across several ones.

B. *IEEE 1609.2*

The scope of this standard includes describing the administrative functions necessary to support the core security operations. Therefore, it specifies the security services offered for applications and WAVE-related management messages.

The considered generic security services are confidentiality, authentication, authorization and integrity. In order to perform the related cryptographic operations (i.e. signature, encryption), the standard assumes public key certificates along with their related private keys. Annex E of this standard comments on the type of certificates considered. Particularly, it is stated that anonymous certificates are not addressed in this revision, as there is the need to trace back malicious parties. However, the use of pseudonyms (introduced as identifiers used by a WAVE device that do not link to its real-world identity) within certificates is mandated by this norm. Each network node (i.e. vehicle or RSU) has to store several keypairs. In order to refer to a concrete keypair, an identifier called Cryptomaterial Handle is used.

In order to manage revocation, Certificate Revocation Lists (CRLs) are in use. They will be considered by the Certificate Management Entity, which will assess the trustworthiness and validity of a given certificate.

As it happens in ISO 21217, this standard does not define the physical security required. Interestingly, it is mentioned that it does not provide primitives that may be used to extract the private key from a Cryptomaterial Handle. This issue implies that this (potentially malicious) action may be performed physically, but no logical mechanisms are offered. As a difference with the aforementioned standard, the use of secure devices (e.g. hardware security module) is not mentioned in this document.

With respect to the information security services, the standard specifies how cryptomaterial must be loaded and used. However, the mention pointed out in the previous paragraph allows discarding that secure storage is provided[2]. Similarly, no indications are given over the security of the context in which cryptographic processing is carried out. Therefore, the existence of secure processing is not ensured. Regarding the potential reliable time source, Annex E clarifies that this document does not impose accuracy requirements for the time source.

VI. Analysis and Discussion

This Section analyzes the different findings introduced in previous sections concerning recent VANET-related contributions and standards. Particularly, Section VI-A shows the relevance of the considered sample of contributions, thus ensuring that it gives an unbiased, broad overview of security

[1] A third document, ISO 13181, was cited in this standard and mentioned as a preliminary work item [46]. However, it has not evolved towards a normative document.

[2] Annex E of this standard also mentions that implementations should protect private keys for being trivially revealed (e.g. stored unencrypted on disk) and for being used in an unauthorized way. In the authors' opinion, this is not a proper requirement for a secure storage environment.

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

trends in this research field. On the other hand, Section VI-B discusses the situation found concerning security models and their compatibility.

A. *Survey relevance*

This survey covers 41 works, which are distributed within the last 6 years. The only exception is paper [16], which is from 2004. It has been selected because of its high impact (more than 270 cites according to Google Scholar). Figure 3 shows the distribution of articles for each year. It may be seen that a representative sample exist for each one.

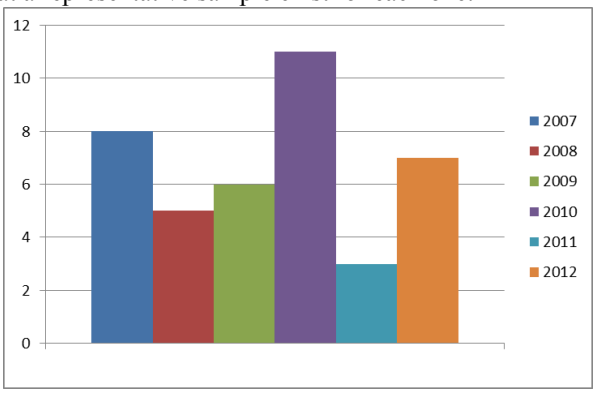

Fig. 3. Distribution of articles per year

Concerning the nature of the analyzed works, it covers both conferences and journals (Figure 4). Particularly, the sample is composed by almost half (23 out of 41) of conferences, being the other half (18 out of 41) formed by journals. Among journals, most of them correspond to indexed ones in Thomson's Journal Citation Report, which is considered as a relevant index for measuring the journal impact. Only one journal is not listed in the aforementioned ranking.

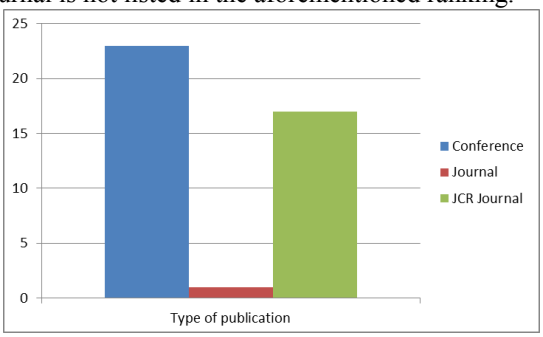

Fig. 4. Distribution of articles per type

To ensure that the selected works cover all aspects of security and privacy, the goal of each approach must be analyzed. For this purpose, the main security requirements, namely anonymity, confidentiality, sender authentication, data integrity, non-repudiation, availability, data trust and privacy have been considered. Other important security requirements such as access control or receiver authentication have been left out of the analysis as they are not usual in recent approaches within this research field. As seen on Figure 5, each service is covered by more than 10 proposals, which seems to be a representative value. The only exception is the availability service, which is explicitly addressed by 3 proposals. Nevertheless, it must be noted that most research efforts in these networks implicitly intend to provide this availability. Computational resources of vehicles, along with the potential bottlenecks in centralized entities, call for lightweight mechanisms.

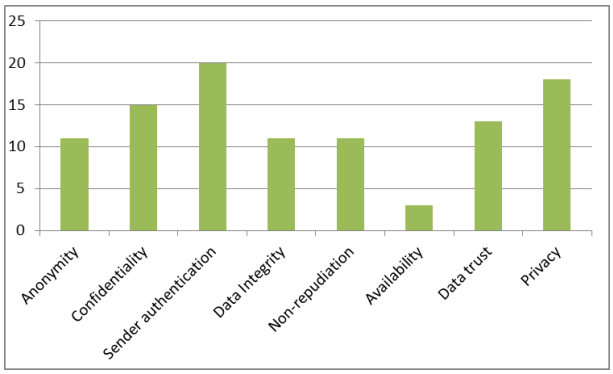

Fig. 5. Distribution of security services covered by the selected articles

B. *Discussion*

Considering the conducted survey, it is clear that a huge amount of different security models have been proposed in recent literature. They are formed by different choices in each of the issues concerning vehicles, RSUs, TTPs and attackers.

Taking into account the revision of the trust in vehicles and RSUs, a key conclusion is that a noteworthy portion of works does not include these considerations. As a consequence, these issues remain unclear and thus it is not possible to perform a holistic security analysis over these proposed mechanisms. Even worse, it may lead to practical, real-world implementations in which vulnerabilities are discovered due to this lack of security specification. Note that these security threats may affect to the provision of services, potentially leading to safety dangers in the vehicles at stake.

Different types of TTPs have been found in the considered works. This fact has two undesirable consequences. On the one hand, some approaches are not benefiting from having more TTPs than those considered. On the other hand, it may happen that the same entity is required to be trusted for one approach whereas it is untrusted for another one. In the latter case, this causes the total incompatibility among proposals.

With respect to attackers, a significant amount of combinations of capabilities, placement and dimension have been found. Even if there are usual capabilities (like eavesdropping or impersonation), other attacks are only sparingly considered. The worst consequence is that in the absence of a complete, holistic security analysis for a given proposal, weaknesses may be found due to the attacker features not considered yet. Even worse, when several approaches are combined and only one of them is protected against a given attack, the resulting combination may be

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

vulnerable. For example, if one proposal prevents tracking but it is not considered by the other one, the result is that tracking may be performed and that protective actions carried out by the first approach are useless.

On the other hand, standards offer a particular choice for several of these components. Thus, standard IEEE 1609.2 calls for the use of public key certificates, which has a direct implication over the required cryptomaterial. Concerning standard ISO 21217, it specifies the use of HSMs which will enable the provision of secure processing and storage. Considering the surveyed works, these decisions are in conflict with assumptions made in some proposals.

Taking into account the previous facts, it may be concluded that there is an urgent need to agree on a set of common settings in order to achieve reliable and interoperable security and privacy services. This situation will lead to a set of enhanced Intelligent Transport System (ITS) services that can co-exist in a single vehicular environment. In this way, efforts taken by researchers and industry will be aligned, thus promoting an earlier and more mature development of ITS environments. Note that without compatibility among their underlying models, different ITS services may not be used at the same time.

VII. Basic approach to compare security models

Considering the discussion presented in Section VI-B, it is necessary to work towards a common (or, at least, compatible) framework for security models in this field.

In order to address this issue, the use of a systematic classification of security models may help to clarify the similarities and differences between contributions. In this way, it will be clearer whether two mechanisms are built over a common set of assumptions, thus ensuring their compatibility. At the same time, it may help on identifying those proposals that, although built on different assumptions, may be co-existent. Furthermore, it will highlight the choices made on each aspect, thus contributing to avoid the lack of decisions over an issue, as it happened in several surveyed works.

Based on the different categories identified along the survey, a simple approach to compare security models is proposed herein. The approach consists in building a comparison chart, in which each row is an analyzed feature (recall Figure 2) and each column represents a given work. Each cell is filled up with the corresponding values for each model feature in the considered proposal. Whenever two cells in a given row contain the same value, they are identified as compatible. This approach enables identifying the points of coincidence and divergence between contributions. Thus, it is a first step to clarify whether these proposals may co-exist or not, or even if they are fully similar or divergent. Enhancing this approach to introduce a fine-grained compatibility measure for those cases in which a given feature is not *exactly* the same among different articles is left to future work.

To illustrate the proposed approach, Table VI compares papers [4], [28] and [34]. In this Table, highlighted cells contain the same value for a given feature. Thus, it may be seen that papers [28] and [34] make the same assumptions over the trust on vehicular devices, whereas this aspect is not defined in [4].

Concerning vehicular credentials, they all tend to a partially distributed creation. Papers [28] and [34] are compatible in that they suppose that the vehicle stores a secret value. Nevertheless, [28] uses pseudonym-based certificates, which may (or may not) harm compatibility depending on the design of [34]. This situation highlights the need for the aforementioned planned enhancement. In any case, it is easy to observe that [28] and [4] are not compatible since the latter uses public key cryptography without certificates.

Regarding RSUs, a common point of these approaches is that they do not consider the existence of these devices. This is the most suitable situation from the compatibility viewpoint.

With respect to the existence of TTPs, this point is especially critical when an approach considers one entity to be trusted while another one does not. As this is not the case in these approaches, this issue does not raise great compatibility concerns. For example, [28] and [4] would be fully compatible if they are deployed in a scenario in which certificate management is supervised by a government-related entity. Even further, the three works could be co-existent (regarding TTPs) if vehicle manufacturers might be trusted without consequences over [28] and [4].

The attacker features are quite different in the studied proposals. Despite the differences on what the attacker can do, it is also noticeable that [34] assumes that it cannot collude. These differences on the attacker features discourage applying these proposals at the same time.

As a consequence of this analysis, it has been shown that the proposed approach simplifies identifying the chance for different mechanisms to co-exist. In this way, it offers a suitable solution for the existing problem.

VIII. Related work

Security issues in vehicular ad-hoc networks have been extensively considered in previous works. As an example, Stampoulis and Chai performed a survey which contains an overview of security requirements, a description on adversaries and their attacks and an introduction to proposed countermeasures [48]. An up-to-date, holistic revision of these issues has been recently published [51]. Our work expands these works in three directions. First, the assumptions on trustworthiness of each node/device in recent works are revised. Second, the security-related considerations in standards are also described. Third, a proposal to compare different contributions regarding their security assumptions (i.e. models) is presented.

Another security-related survey focused on the usual security requirements, their associated threats and the proposed contributions to successfully achieve these

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

requirements [49]. The work presented herein complements their vision – whereas that paper gives an overview on the set of proposed approaches, this survey focuses on the set of assumptions (i.e. underlying models) that form the basis of these approaches. It must be noted that without a clear vision on their assumptions, it is not easy to identify which approaches can be simultaneously applied.

IX. Conclusions and Future Work

Several elements compose the complex scenario of vehicular networks. Over these elements, different assumptions can be made to build a proposal (e.g. a mechanism, a protocol, a service, etc.). These assumptions form its underlying model. Given the significant amount of Intelligent Transport Systems services that may be offered at the same time within a single network, it is necessary to ensure that their models are compatible each other. This work has focused on security-related models. Thus, a survey of the models of 41 security-related works in vehicular networks has been presented. This survey has focused on the assumptions performed over the vehicular devices, Road-Side Units (RSUs), Trusted Third Parties and the attacker features.

The analysis has shown the degree of differences existing in the revised works, thus leading to the undesirable scenario in which they cannot co-exist. Even worse, it has been identified that a significant portion of contributions do not clarify key aspects such as the trust of vehicular devices or RSUs. The view from the standards states the current technical mandates that should apply on each aspect. The analysis has shown that it contradicts usual assumptions on the revised proposals. Therefore, this survey aims to raise awareness on this issue in order to bring together standards and fully specified technical-scientific contributions.

In order to highlight the similarities and differences between models, a simple comparison approach has also been proposed. It gives an easy way to identify conflicting aspects, as a first step to solve them.

Future work on this area will have two main directions. On the one hand, the amount of elements analyzed in this survey will be extended, introducing other issues that may have an impact over the global security. For example, the revocation management of vehicular credentials or the assumptions on RSUs interconnection will be studied. On the other hand, a measure of similarity will be designed to improve the proposed comparison mechanism. Thus, it will be possible to determine whether two proposals may co-exist even if they rely upon different security assumptions.

Appendix

TABLE I
TRUST ON VEHICULAR DEVICES. HIGHLIGHTED ROWS DO NOT ADDRESS THIS ISSUE

	1.1. Type of device			**1.2. Features**		
	1.1.0. Untrusted	**1.1.1. Tamper-proof**	**1.1.2. Tamper-resistant**	**1.2.1. Reliable crypto**	**1.2.2. Reliable storage**	**1.2.3. Reliable time source**
[1]			x	x	x	
[2]		x				
[3]	x					
[4]						
[5]		x		x	x	
[6]						
[7]	x					
[8]						
[9]						
[10]		x		x	x	x
[11]		x			x	
[12]			x			
[13]						
[14]						
[15]						
[16]						
[17]						
[18]			x	x	x	
[19]						
[20]						
[21]						x
[22]						
[23]						
[24]						x
[25]			x	x	x	
[26]		x				
[27]			x	x	x	
[28]			x	x	x	x
[29]						
[30]		NO	NO			
[31]						
[32]						
[33]						
[34]			x	x	x	x
[35]			x		x	
[36]						
[37]						
[38]						
[39]						
[40]						
[41]		x		x	x	

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

TABLE II
VEHICULAR CREDENTIALS. HIGHLIGHTED ROWS DO NOT ADDRESS THIS ISSUE

	2.1. Creation				2.2. Nature										
	2.0. None	2.1.1. Centra-lized	2.1.2. Partial distrib. (vehicles, RSU)	2.1.3. Fully by vehicles	2.2.1. Single identif.	2.2.2. Pseudo-nyms	2.2.3. Public key crypto			2.2.4. ID-based credential	2.2.5. Attrib.-based crypto	2.2.6. Vehicular secret value	2.2.7. Session key	2.2.8. Group key
							2.2.3.1. Certif. (pseud.)	2.2.3.2. Certif. (anony.)	2.2.3.3 No certif.					
[1]			x		x	x						x		
[2]			x											x
[3]														
[4]			x		x				x					
[5]				x		x			x				x	
[6]			x				x							
[7]		x					x							
[8]			x							x				
[9]			x					x						
[10]		x			x				x				x	
[11]			x		x			x			x			
[12]				x	x			x						
[13]			x						x					
[14]			x						x					
[15]				x	x									
[16]				x		x			x					
[17]			x		x		x		x					x
[18]		x			x		x							
[19]		x					x							
[20]		x			x									x
[21]										x				
[22]			x		x	x								x
[23]				x									x	x
[24]		x			x		x							
[25]		x					x							
[26]		x			x		x						x	
[27]			x		x		x						x	
[28]			x				x					x		
[29]				x					x					
[30]		x									x			
[31]			x		x		x							
[32]			x								x			
[33]		x			x		x							
[34]			x									x		
[35]		x			x		x							
[36]		x					x							
[37]				x			x							
[38]														
[39]		x					x							
[40]			x		x							x		
[41]			x								x	x		

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

TABLE III
TRUST ON RSUS. HIGHLIGHTED ROWS DO NOT ADDRESS THIS ISSUE

	3.0 Absent	3.1 Type of device			3.2 Features		
		3.1.0. Un-trusted	3.1.1. Tam-per-proof	3.1.2. Tamper -resist	3.2.1. Reliab crypto	3.2.2. Reliab. storage	3.2.3. Reliab. time source
[1]							
[2]							
[3]	x						
[4]	x						
[5]							
[6]	x						
[7]					x	NO	
[8]			x			x	
[9]		x				x	
[10]				x	x	x	x
[11]				x	x	x	x
[12]							
[13]			x		x	x	
[14]		x					
[15]	x						
[16]	x						
[17]							
[18]							
[19]	x						
[20]							
[21]		x					
[22]							
[23]	x						
[24]							
[25]	x						
[26]					x		
[27]				x	x	x	x
[28]	x						
[29]	x						
[30]	x						
[31]							
[32]				x	x	x	x
[33]							
[34]	x						
[35]	x						
[36]		x					
[37]							
[38]							
[39]				x	x	x	x
[40]							
[41]			x	x	x	x	x

TABLE IV
CONSIDERED TRUSTED THIRD PARTIES (TTPS)

	4.0. None	4.1. Certif-related auth.	4.2. Gover-nment-related auth	4.3. VANET -related Auth. (e.g. group mngr.)	4.4. Generic trusted auth.	4.5. Serv. prov.	4.6. Veh. manuf.
[1]		x	x		x		
[2]		x		x			
[3]	x						
[4]			x				
[5]					x		
[6]		x			x		
[7]			x				
[8]			x		x		
[9]					x		
[10]					x		
[11]					x		
[12]		x					
[13]		x					
[14]		x			x		
[15]		NO					
[16]	x						
[17]		x					
[18]		x					
[19]		x					
[20]		x	x	x			
[21]		x					
[22]	x						
[23]				x			
[24]		x					
[25]		x					
[26]		x				x	
[27]					x		
[28]		x					
[29]	x						
[30]		x					
[31]		x					
[32]					x		
[33]		x					
[34]			x				x
[35]		x			x		
[36]		x					
[37]		x					
[38]	x						
[39]		x					
[40]					x		
[41]		x					

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

TABLE V
ATTACKER MODEL. HIGHLIGHTED ROWS DO NOT ADDRESS THIS ISSUE

	5.1. Capabilities						5.2. Scope: Nature		5.3. Scope:Dimension		
	5.1.1. Eavesdrop /tracking	**5.1.2. Modify / Forge / Erase**	**5.1.3. Inject / Replay**	**5.1.4. Impersonate /Identity manipulation**	**5.1.5. Jam**	**5.1.6. Credential stealing / OBU hacking**	**5.2.1. Vehicle**	**5.2.2. RSU**	**5.3.1. Can collude**	**5.3.2. Honest majority**	**5.3.3. Global coverage**
[1]	x	x			x						
[2]	x	x									
[3]		x	NO								
[4]				x							
[5]				x						x	
[6]			x	x					x	x	
[7]	x		x	x			x		x		x
[8]											
[9]	x			x							
[10]	x										
[11]	x	x	x	x							x
[12]	x	x	x								
[13]	x	x	x	x			x				x
[14]		x	x	x							
[15]	x			x							
[16]			x	x					x		
[17]				x							
[18]		x	x		x				x	x	
[19]			x								
[20]	x	x	x	x							x
[21]			x	x				x			
[22]	x										
[23]	x			x							
[24]		x	x		x					x	
[25]		x	x								
[26]											
[27]	x			x							
[28]	x			x							
[29]		x	x		x		x		x	x	
[30]				x		x			x		
[31]			x	x							
[32]	x	x	x		x						
[33]	x					x					
[34]	x	x	x					x	NO	x	
[35]	x				NO	NO	x				
[36]				x							
[37]	x					x					
[38]		x	x				x				
[39]	x								x		
[40]	x			x	x						
[41]				x		x	x		x		

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

TABLE VI
COMPARISON OF SECURITY MODELS BASED ON SURVEYED FEATURES. HIGHLIGHTED CELLS CONTAIN THE SAME VALUES

	[28]	[34]	[4]
Trust on vehicular device	1.1.2 (tamper-resistant); 1.2.1. (reliable crypto); 1.2.2. (reliable storage); 1.2.3. (reliable time source)	1.1.2 (tamper-resistant); 1.2.1. (reliable crypto); 1.2.2. (reliable storage); 1.2.3. (reliable time source)	*Undefined*
Vehicular credentials	2.1.2. (Partially distributed creation (in vehicles, RSUs)) ; 2.2.3.1. (Public key crypto with certif (pseudonym)) ; 2.2.6. (Vehicular secret value)	2.1.2. (Partially distributed creation (in vehicles, RSUs)); 2.2.6. (Vehicular secret value)	2.1.2. (Partially distributed creation (in vehicles, RSUs)); 2.2.1. (Single identifier); 2.2.3.3. (Public key crypto without certif)
Trust on RSU	3.0. (absent)	3.0. (absent)	3.0. (absent)
TTPs	4.1. (Certificate-related authority)	4.2. (Government-related authority); 4.6. (Veh. manufacturer)	4.2.(Government-related authority)
Attacker features	5.1.1. (Eavesdrop / tracking) ; 5.1.4. (Impersonate / Identity manipulation)	5.1.1. (Eavesdrop / tracking) ; 5.1.2. (Modify/Forge/Erase); 5.1.3. (Inject / Replay); 5.2.2. (RSU); NOT 5.3.1 (collusion); 5.3.2. (Honest majority)	5.1.4. (Impersonate / Identity manipulation)

ACKNOWLEDGMENT

Authors would like to thank the anonymous reviewers for their helpful comments that enabled to improve this paper.

REFERENCES

[1] K. Ploessl, and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks", Computer Standards and Interfaces, vol. 30, pp. 390-397, August 2008.

[2] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications", IEEE Transactions on Vehicular Technology, vol. 59, pp. 1606-1617, May 2010.

[3] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET", IEEE Transactions on Vehicular Technology, vol. 61, pp. 275-285, January 2012.

[4] J. Choi, and S. Jung, "Security framework with strong nonrepudiation and privacy in VANETs" in Proceedings of the 6th Annual IEEE Consumer Communications and Networking Conference, Las Vegas, January 2009, pp. 1-5.

[5] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks", IEEE Transactions on Vehicular Technology, vol. 60, pp. 248-262, January 2011.

[6] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "AEMA: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad-hoc networks" in IEEE International Conference on Communications, Beijing, May 2008, pp. 1436-1440.

[7] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET", IEEE Journal on Selected Areas in Communications, vol. 25, pp. 1569-1589, October 2007.

[8] J. Sun, C. Zhang, and Y. Fang, "An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks" in Military Communications Conference, Orlando, October 2007, pp. 1 – 7.

[9] Y. Park, C. Sur, C. D. Jung, and K.-H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications", Journal of Information Science and Engineering, vol. 26, pp. 785-800, May 2010.

[10] N.-W. Wang, Y.-M. Huang, and W.-M. Chen, "A novel secure communication scheme in vehicular ad hoc networks", Computer Communications, vol. 31, pp. 2827-2837, July 2008.

[11] D. Huang, and M. Verma, "ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks", Ad Hoc Networks, vol. 7, pp. 1526-1535, November 2009.

[12] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication" in Communication in Distributed Systems (KiVS), Bern, March 2007, pp. 1-12.

[13] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support" in Military Communications Conference, Boston, October 2009, pp. 1-7.

[14] S. Biswas, and J. Mi i , "Deploying proxy signature in VANETs" in Global Telecommunications Conference, Miami, December 2010, pp. 1-6.

[15] C.-H. Yeh, Y.-M. Huang, T.-I. Wang, and H.-H. Chen, "DESCV: a secure wireless communication scheme for vehicle ad hoc networking", Mobile Networks and Applications, vol. 14, pp. 611-624, October 2009.

[16] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs" in ACM international workshop on Vehicular ad hoc networks, Philadelphia, October 2004, pp. 29-37.

[17] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET" in ACM international workshop on Vehicular ad hoc networks, Montreal, September 2007, pp. 19-28.

[18] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks", IEEE Journal on Selected Areas in Communications, vol. 25, pp. 1557-1568, October 2007.

[19] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, "FAMIC - Fast Authentication and Message Integrity Check" in Security and Cooperation in Wireless networks, Lausanne, 2007.

[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, pp. 3442-3456, November 2007.

This paper has been accepted for publication in IETE Technical review, November-December 2013 issue. Please check out the publisher version at http://tr.ietejournals.org/. Posted with permission of the Editor-in-Chief

[21] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks" in International Conference on Distributed Computing Systems Workshops, Minneapolis, June 2011, pp. 323-331.
[22] P. Cencioni, and R. Di Pietro, "A mechanism to enforce privacy in vehicle-to-infrastructure communication", Computer Communications, vol. 31, pp. 2790-2802, July 2008.
[23] D. Kim, J. Choi, and S. Jung, "Mutual identification and key exchange scheme in secure VANETs based on group signature" in Consumer Communications and Networking Conference, Las Vegas, January 2010, pp. 1-2.
[24] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks" in IEEE Conference on Computer Communications, Phoenix, April 2008, pp. 1238-1246.
[25] E. Schoch, and F. Kargl, "On the efficiency of secure beaconing in VANETs" in ACM conference on Wireless network security, Hoboken, March 2010, pp. 111-116.
[26] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "PAACP: a portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks", Computer Communications, vol. 34, pp. 447-456, March 2011.
[27] V. Paruchuri, and A. Durresi, "PAAVE: protocol for anonymous authentication in vehicular networks using smart cards" in Global Telecommunications Conference, Miami, December 2010, pp. 1-5.
[28] G. Kounga, T. Walter, and S. Lachmund, "Proving the reliability of anonymous information in VANETs", IEEE Transactions on Vehicular Technology, vol. 58, pp. 2977-2989, July 2009.
[29] B. Aslam, S. Park, C.-C. Zou, and D. Turgut, "Secure traffic data propagation in vehicular ad hoc networks", International Journal of Ad Hoc and Ubiquitous Computing, vol. 6, pp. 24-39, July 2010.
[30] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption", in IFIP Annual Mediterranean Ad Hoc Networking Workshop, Juan Les Pins, June 2010, pp. 1-8.
[31] H. Xiong, Z. Qin, and F. Li, "Secure vehicle-to-roadside communication protocol using certificate-based cryptosystem", IETE Technical Review, vol. 27, pp. 214-219, April 2010.
[32] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: situation-aware trust architecture for vehicular networks" in International workshop on Mobility in the evolving internet architecture, Seattle, August 2008, pp. 31-36.
[33] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, "Support of anonymity in VANETs-putting pseudonymity into practice" in Wireless Communication and Networking Conference, Kowloon, March 2007, pp. 3400-3405.
[34] L. Chen, S. Ng and G. Wang. 'Threshold anonymous announcement in VANETs'. Selected Areas in Communications, 29(3). 2011. Retrieved from http://ieeexplore.ieee.org/xpls/abs_ all.jsp?arnumber=5719272
[35] F. Schaub, *et al.* 'V-tokens for Conditional Pseudonymity in VANETs'. Wireless Communications and Networking Conference (WCNC), 2010. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5506126
[36] M. Almulla, *et al.* 'An efficient k -Means authentication scheme for ad hoc networks'. Wireless communications and mobile computing. 2012. doi:10.1002/wcm
[37] A. Bhattacharya, A. Das and D. Roychoudhury. 'Autonomous Certification with List-based Revocation for Secure V2V Communication'. Proc. ICISS. 2012. Retrieved from http://cse.iitkgp.ac.in/~abhij/publications/PKI++.pdf
[38] Y.-C. Wei, and Y.-M. Chen. 'An Efficient Trust Management System for Balancing the Safety and Location Privacy in VANETs'. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012. doi:10.1109/TrustCom.2012.79
[39] J. Almeida, *et al.* 'Probabilistic Key Distribution in Vehicular Networks with Infrastructure Support'. Proc. IEEE Globecom. 2012. Retrieved from http://www.contrib.andrew.cmu.edu/~mboban/jalmeida_ globecom2012.pdf
[40] U. Singh and P. Singh. 'Security and Privacy Enabling Solution for Vehicular Networks'. Signal Processing and Information Technology. 2012. Retrieved from http://www.springerlink.com/index/H151R63714127826.pdf
[41] S. Karumanchi, A.Squicciarini and D. Lin. 'Selective and Confidential Message Exchange in Vehicular Ad Hoc Networks'. International Conference on Network and System Security (NSS). 2012. Retrieved from http://personal.psu.edu/users/s/i/sik5273/NSS2012/TechReport.pdf
[42] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Std 1609.2-2006
[43] ISO 21217:2010, Intelligent transport systems -- Communications access for land mobiles (CALM) -- Architecture.
[44] ISO/TR 11766:2010, Intelligent transport systems - Communications access for land mobiles (CALM) - Security considerations for lawful interception
[45] ISO/TR 11769:2010, Intelligent transport systems - Communications access for land mobiles (CALM) - Data retention for law enforcement
[46] Convenor's report ISO TC204-WG16. Available at: http://ftp.tiaonline.org/iso_ tc204/New_Orleans/WG16/Report/WG2016/Convenor's Report-New Orleans final (4).ppt
[47] P. Papadimitratos, *et al.* 'Secure vehicular communication systems: design and architecture'. Communications Magazine, IEEE, 46 (11), 2008.
[48] A. Stampoulis, Z. Chai, A survey of security in vehicular networks. Available at: http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf
[49] J.M. de Fuentes, A. I. Gonzalez-Tablas and A. Ribagorda. Overview of security issues in Vehicular Ad-hoc Networks. Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts IGI Global, 2011.
[50] M. Wolf, A. Weimerskirch and C. Paar. 'Security in automotive bus systems' in Proc. 2nd Workshop on Embedded Security in Cars (ESCAR), 2004.
[51] M.A Moharrum, and A.A.A Daraiseh, "Toward Secure Vehicular Ad-hoc Networks: A Survey," IETE Technical Review, Vol. 29, no. 1, pp. 80-9, 2012.
[52] R.S. Zuberi, B. Lall, and S.N. Ahmad, "Privacy Protection Through k-anonymity in Location-based Services," IETE Technical Review, Vol. 29, no. 3, pp. 196-201, 2012.

Jose Maria de Fuentes, Ph.D. is teaching assistant in the Computer Science and Engineering Department at University Carlos III of Madrid (Spain). His main research interests are digital evidences management, non-repudiation issues and secure message distribution in vehicular environments. He has published several articles in international conferences and journals. He is part of the research team of the Spanish national R+D project E-SAVE, which is focused on VANET evidence management and automated road traffic enforcement processes.

Lorena Gonzalez-Manzano is Ph.D. candidate and teaching assistant in the Computer Science and Engineering Department at University Carlos III of Madrid (Spain). She received the Master in Computer Science and Technology degree in February 2012 from the same University. Her main research interests are security and privacy in social networks. She has published several papers in national and international conferences.

Ana Isabel Gonzalez-Tablas is associate professor in the Computer Science and Engineering Department at University Carlos III of Madrid. She received her Ph.D. degree in Computer Science from University Carlos III of Madrid, Spain, in 2005. Her main research interests are security and privacy for Intelligent Transportation Systems and Location Based Services. She has published numerous articles in international journals and conferences.

Jorge Blasco is teaching assistant of the Computer Security Laboratory Research Group at the Computer Science Department of the Carlos III University of Madrid. He obtained his Ph. D. at the same University in June 2012. Blasco has published several research papers on international journals and conferences. His main research interests are data leakage protection technologies and steganography.