This chapter/paper appears in **Handbook of Research on Mobility and Computing**

edited by **Maria Manuela Cruz-Cunha** and **Fernando Moreira**.

Overview of security issues in Vehicular Ad-hoc Networks

José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda

Department of Computer Science

University Carlos III of Madrid (Spain)

Corresponding author: jfuentes@inf.uc3m.es

ABSTRACT

Vehicular ad-hoc networks (VANETs) are a promising communication scenario. Several new applications are envisioned, which will improve traffic management and safety. Nevertheless, those applications have stringent security requirements, as they affect road traffic safety. Moreover, VANETs face several security threats. As VANETs present some unique features (e.g. high mobility of nodes, geographic extension, etc.) traditional security mechanisms are not always suitable. Because of that, a plethora of research contributions have been presented so far. This chapter aims to describe and analyze the most representative VANET security developments.

KEYWORDS

Vehicular ad-hoc networks (VANET), security, authentication, privacy, non-repudiation, confidentiality, availability, data trust, attacks.

INTRODUCTION

Nowadays, road traffic activities are one of the most important daily routines worldwide. Passenger and freight transport are essential for human development. Thus, new improvements on this area are achieved every day - better safety mechanisms, greener fuels, etc.

Driving is one of the most incident factors of traffic safety, so there is a clear need to make it safer. Apart from partially automating this task, reliable driver data provisioning is critical to achieve this goal. An accurate weather description or early warnings of upcoming dangers (e.g. bottlenecks, accidents) would be highly useful for drivers. For this purpose, a new kind of information technology called **VANET** (**V**ehicular **A**d-hoc **NET**work) is being developed.

VANETs are a subset of MANETs (Mobile Ad-hoc NETworks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications). Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads.

Data interchanged over VANETs often play a vital role in traffic safety. For example, in the eCall project, an emergency call is made once in-vehicle sensors detect that an accident has occurred (eSafetySupport, 2007). Such information must be accurate and truthful, as lives could depend on this application. In this way, very stringent security requirements are to be achieved. Moreover, privacy of drivers should be protected – a vehicle should not be easily tracked by

unauthorized entities. Satisfying all these security requirements have lead to a great amount of research contributions, each one covering different aspects of data security and privacy.

This chapter offers an overview of the current status of security issues over VANETs. For this purpose, different communication models have been identified and analyzed from the security point of view. Moreover, security requirements and potential attacks will be studied. Finally, the security developments to achieve such requirements will be analyzed. In this way, the reader will identify the current trends in data security proposed to solve not only traditional problems (e.g. data confidentiality) but also some context-specific ones (e.g. eviction of misbehaving vehicles from the VANET).

Chapter organization. On Section II, a typical VANET model is explained, covering the existing entities and their relationships. Different communication models will be identified as well. Section III presents the security requirements that must be achieved in VANETs and particularly in each communication model. Section IV shows a classification of attacks identified on VANETs. Section V analyzes the main security mechanisms proposed to achieve the security requirements previously introduced. Finally, Section VI sums up the main conclusions and lessons learned from this work, and points out future research directions on VANET security.

VANET MODEL OVERVIEW

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. In this Section we will firstly describe the most common entities that appear in VANETs. In the second part, we will analyze the different VANET settings that can be found among vehicles, and among vehicles and the remaining entities.

Common VANET entities

Several different entities are usually assumed to exist in VANETs. To understand the internals and related security issues of these networks, it is necessary to analyze such entities and their relationships. Figure 1 shows the typical VANET scheme.

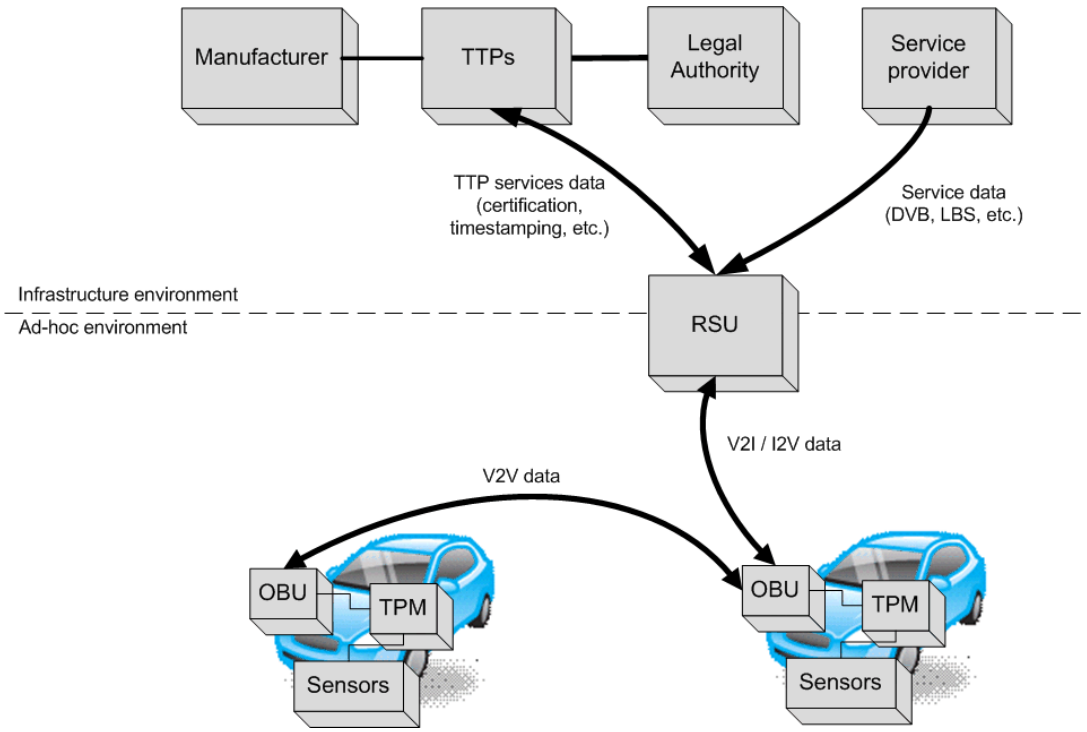

Figure 1. Simplified VANET model

As seen on Figure 1, two different environments are generally considered in VANETs:

- **Infrastructure environment**. In this part of the network, entities can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. On one hand, **manufacturers** are sometimes considered within the VANET model. As part of the manufacturing process, they identify uniquely each vehicle. On the other hand, the **legal authority** is commonly present in VANET models. Despite the different regulations on each country, it is habitually related to two main tasks - *vehicle registration* and *offence reporting*. Every vehicle in an administrative region should get registered once manufactured. As a result of this process, the authority issues a license plate. On the other hand, it also processes traffic reports and fines. Trusted Third Parties (**TTP**) are also present in this environment. They offer different services like credential management or timestamping. Both manufacturers and the authority are related to TTPs because they eventually need their services (for example, for issuing electronic credentials). **Service providers** are also considered in VANETs. They offer services that can be accessed through the VANET. Location-Based Services (LBS) or Digital Video Broadcasting (DVB) are two examples of such services.
- **Ad-hoc environment**. In this part of the network, sporadic (ad-hoc) communications are established from **vehicles**. From the VANET point of view, they are equipped with three different devices. Firstly, they are equipped with a communication unit (**OBU**, On-Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of **sensors** to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance). These sensorial data can be shared with other vehicles to increase their awareness and improve road safety. Finally, a Trusted Platform Module (**TPM**) is often mounted on vehicles. These devices are especially interesting for security purposes, as they offer reliable storage and computation. They usually have a reliable internal clock and are supposed to be tamper-resistant or at least tamper-evident (Papadimitratos, Buttyan, Hubaux, Kargl, Kung, & Raya, 2007). In this way, sensitive information (e.g. user credentials or pre-crash information) can be reliably stored.

As mentioned before, VANETs as communications network impose several unique requirements. Vehicles move at a relatively high speed and, on the other hand, the high amount of vehicles present in a road could lead to an enormous network. Thus, a specific communication standard, called Dedicated Short Range Communications (DSRC) has been developed to deal with such requirements (Armstrong Consulting Inc.). This standard specifies that there will be some communications devices located aside the roads, called Road-Side Units (**RSU**). In this way, RSUs become gateways between the infrastructure and vehicles and vice versa.

VANET settings

Several applications are enabled by VANETs, mainly affecting road safety. Within this type of application, messages interchanged over VANETs have different nature and purpose. Taking this into account, four different communication patterns (depicted on Figure 2) can be identified:

- **V2V warning propagation (Fig. 2-a)**. There are situations in which it is necessary to send a message to a specific vehicle or a group of them. For example, when an accident is detected, a warning message should be sent to arriving vehicles to increase traffic safety. On the other hand, if an emergency public vehicle is coming, a message should be sent for preceding vehicles. In this way, it would be easier for the emergency vehicle to have a free way. In both cases, a routing protocol is then needed to forward that message to the destination.

- **V2V group communication (Fig. 2-b)**. Under this pattern, only vehicles having some features can participate in the communication. These features can be static (e.g. vehicles of the same enterprise) or dynamic (e.g. vehicles on the same area in a time interval).
- **V2V beaconing (Fig. 2-c)**. Beacon messages are sent periodically to nearby vehicles. They contain the current speed, heading, braking use, etc. of the sender vehicle. These messages are useful to increase neighbor awareness. Beacons are only sent to 1-hop communicating vehicles, i.e. they are not forwarded. In fact, they are helpful for routing protocols, as they allow vehicles to discover the best neighbor to route a message.
- **I2V/V2I warning (Fig. 2-d)**. These messages are sent either by the infrastructure (through RSUs) or a vehicle when a potential danger is detected. They are useful for enhancing road safety. As an example, a warning could be sent by the infrastructure to vehicles approaching to an intersection when a potential collision could happen.

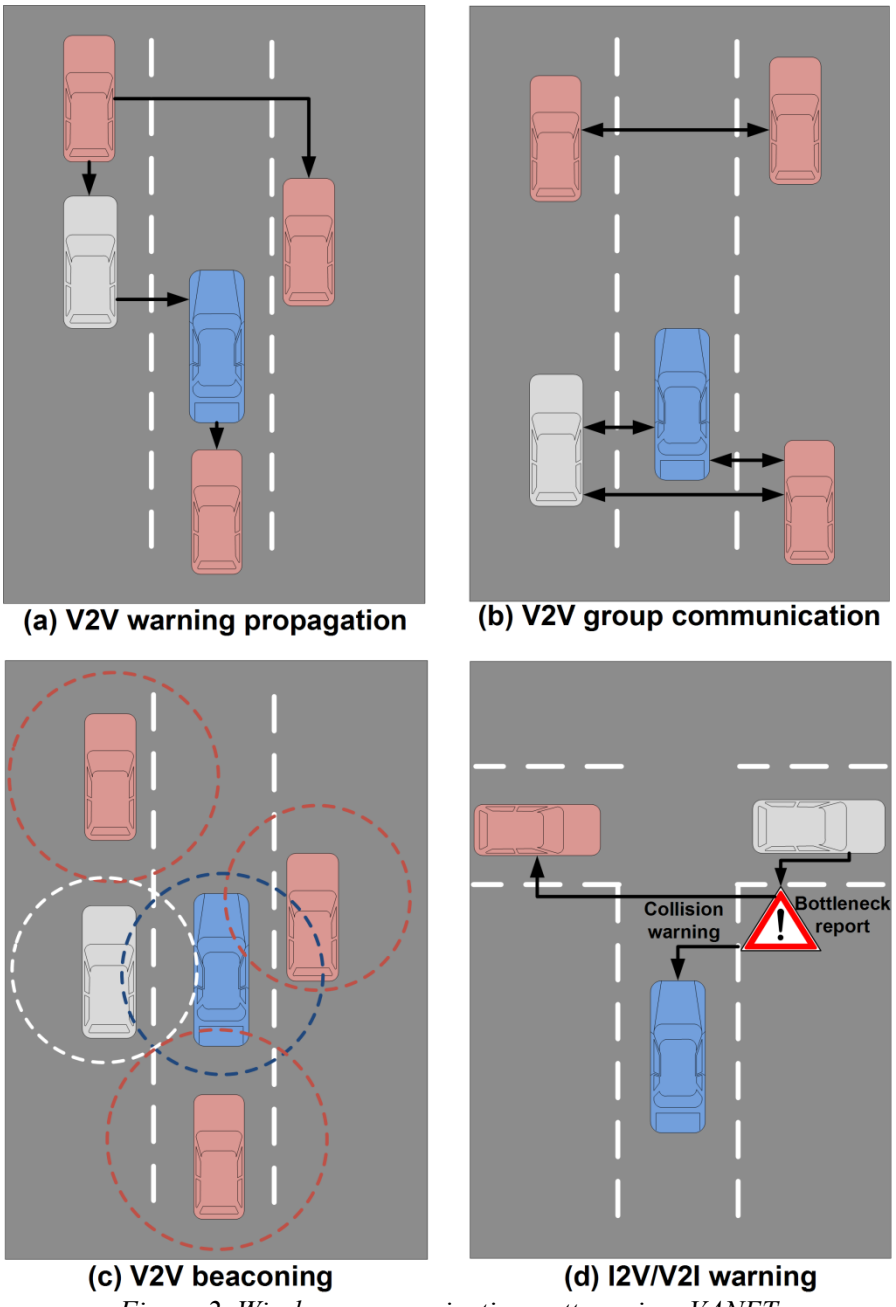

Figure 2. Wireless communication patterns in a VANET

There exist other communication patterns over VANETs (e.g. related to multimedia access, location-based services, etc.). In particular, vehicles could use different communication media like cellular networks (e.g. GSM/GPRS) to get such services. However, we will focus on V2V and V2I road safety communication patterns over VANETs, as they will be more challenging from the security point of view. In fact, each communication pattern has a different set of security requirements. This matter will be analyzed on the next Section.

SECURITY REQUIREMENTS FOR VANETS

Taking into account the different entities and data at stake, in this Section a catalog of security requirements is built. Table 1 specifies the identified security requirements for each VANET setting introduced on the previous Section. Although I2V and V2I were considered to be the same setting, they have different security requirements and so they have been distinguished here.

Table 1. Security requirements for each VANET setting

VANET setting / Sec. Requirement	V2V warning propagation	V2V group communication	V2V beaconing	I2V warning	V2I warning
Entity identification	✓ *(all vehicles)*	×	✓ *(sender)*	✓ *(sender)*	✓ *(sender&receiver)*
Entity authentication	✓ *(sender)*	×	✓ *(sender)*	✓ *(sender)*	✓ *(sender&receiver)*
Attribute authentication	×	✓ *(sender&receiver)*	×	×	×
Privacy preservation	✓	✓	✓	×	✓
Non-repudiation	✓ *(sender)*	×	✓ *(sender)*	✓ *(sender&receiver)*	✓ *(sender&receiver)*
Confidentiality	×	✓	×	×	×
Availability	✓	✓	✓	✓	✓
Data trust	✓	✓	✓	✓	✓

First of all, **entity identification** imposes that each participating entity should have a different and unique identifier. However, identification itself does not imply that the entity proves that it is its actual identity – this requirement is called **entity authentication**. Each of the application groups (enabled by the communication patterns previously introduced) has different needs regarding to these requirements. V2V warning propagation needs identification to perform message routing and forwarding – identifiers are essential to build routing tables. Sender authentication is also needed for liability purposes. Imagine that a regular vehicle sends a notification as if it were a police patrol. It should be then needed to prove the identity of the emitting node. In group communications it is not required to identify or authenticate the communicating peers. The only need is to show that both participating entities have the required attributes to become group members – this is the **attribute authentication** requirement. In fact, this is the only communication pattern that needs this requirement. In beaconing, identification and authentication of the sender is needed. Nearby vehicles can then build a reliable neighbor table. Both requirements are also present in I2V warnings, where only messages sent by the infrastructure are credible. Infrastructure warnings are sent to all passing vehicles within an area, so identification or authentication of the receiver is not needed. On the contrary, V2I warnings also require the emitting vehicle to be identified and authenticated. In this way, only vehicles with a trustworthy identity will be able to send such messages.

Accomplishing the cited requirements should not imply less privacy. In fact, **privacy preservation** is critical for vehicles. In the vehicular context, privacy is achieved when two related goals are satisfied – ***untraceability*** and ***unlinkability*** (Gerlach, 2005). First property

states that vehicle´s actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, second property establishes that it should be impossible for an unauthorized entity to link a vehicle´s identity with that of its driver/owner. However, this privacy protection should be removed when required by traffic authorities (i.e. for liability attribution). This requirement is present in all V2V communications. In fact, privacy should not get compromised even if different messages (no matter if under different communication patterns) are sent by the same vehicle. It does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes. In group communications it is not generally required, as the emitting node could be any of the group members. With respect to I2V and V2I warnings, non-repudiation of origin is needed, so wrong warning messages can be undoubtedly linked to the sending node. Non-repudiation of receipt is not currently needed, but it will be in the future. Currently, accident responsibility relies only on the human driver. However, in the future there are some envisioned applications that would automate partially the driving task. In such situation, not receiving a warning message could be critical for liability attribution.

Another important security requirement in vehicular communications is **confidentiality**, that is, to assure that messages will only be read by authorized parties. This requirement is only present in group communications, in which only group members are allowed to read such information. The remaining VANET settings transmit public information. In fact, this requirement is not considered in some previous works (Lin, Sun, Ho, & Shen, 2007). Nevertheless, for the sake of completeness, it will be taken into account in this overview.

The **availability** requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and mechanisms should save as much bandwidth and computational power as possible, while fulfilling these security requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also I2V ones.

Finally, related to the information itself, data integrity and accuracy must be assured. Both needs are globally referred as **data trust**. Data at stake should not be altered and, more importantly, it should be truthful. It also implies that received information is fresh (i.e. refers to the current state of the world). False or modified data should lead to potential crashes, bottlenecks and other traffic safety problems. For this reason, data trust must be provided on all VANET communications.

OVERVIEW OF ATTACKS IN VANETS

Once the security requirements have been established for VANETs, many attacks can be identified to compromise them (Aijaz, et al., 2006). In this Section we elaborate on these attacks, explaining how they can be performed and their potential consequences. For the sake of clarity, attacks have been classified depending on the main affected requirement.

Attacks on identification and authentication

There are two main attacks related to identification and authentication:

- **Impersonation.** The attacker pretends to be another entity. It can be performed by stealing other entity´s credential. As a consequence, some warnings sent to (or received by) a specific entity would be sent to (or received by) an undesired one.
    - **False attribute possession**. This is a subtype of impersonation, in which the attacker tries to show the possession of an attribute (e.g. to be a member of an enterprise) to get some benefit. It could be performed if false credentials could be built, or if revoked credentials could be used normally. As a consequence, a regular vehicle could send messages claiming to be a police patrol, letting it to have a free way.

- **Sybil**. The attacker uses different identities at the same time. In this way, a single vehicle could report the existence of a false bottleneck.

As presented in the VANET model, TPMs mounted on vehicles can store sensitive information like identifiers. In this way, the Sybil threat is alleviated. However, security mechanisms must be designed to provide identification and authentication, thus protecting against impersonation attacks.

Attacks on privacy

Attacks on privacy over VANETs are mainly related to illegally getting sensitive information about vehicles. As there is a relation between a vehicle and its driver, getting some data about a given vehicle´s circumstances could affect its driver privacy. These attacks can then be classified attending to the data at risk:

- **Identity revealing**. Getting the owner´s identity of a given vehicle could put its privacy at risk. Usually, a vehicle´s owner is also its driver, so it would simplify getting personal data about that person.
- **Location tracking**. The location of a vehicle in a given moment, or the path followed along a period of time are considered as personal data. It allows building that vehicle´s profile and, therefore, that of its driver.

Mechanisms for facing both attacks are required in VANETs. They must satisfy the tradeoff between privacy and utility. In this way, security mechanisms should prevent unauthorized disclosures of information, but applications should have enough data to work properly.

Attacks on non-repudiation

The main threat related to non-repudation is denying some action by some of the implicated entities. Non-repudiation can be circumvented if two or more entities share the **same credentials**. This attack is different from the *impersonation* attack described before – in this case, two or more entities collude to have a common credential. In this way, they get indistinguishable, so their actions can be repudiated.

Credential issuance and management should be secured in VANETs to alleviate this threat. Although reliable storage has been assumed in vehicles (by their TPMs), having identical credentials in different vehicles should be avoided. Moreover, mechanisms that provide a proof of participation have to be also implemented.

Attacks on confidentiality

Eavesdropping is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

Attacks on availability

As any other communication network, availability in VANETs should be assured both in the communication channel and in participating nodes. A classification of these attacks, according to their target, is as follows:

- **Network Denial of Service (DoS)**. It overloads the communication channel or makes its use difficult (e.g. interferences). It could be performed by compromising enough RSUs, or by making a vehicle to broadcast infinite messages in a period of time.
    - **Routing anomalies.** It is a particular case of network attack that could lead to a DoS. In this case, attackers don´t participate correctly in message routing over the network. They drop all received messages (**sinkhole attack**) or just a few ones according with their interests (**selfish behavior**).

- **Computation DoS**. It overloads the computation capabilities of a given vehicle. Forcing a vehicle to execute hard operations, or to store too much information, could lead to this attack.

Attacks on data trust

Data trust can be compromised in many different ways in VANETs. **Inaccurate data calculation and sending** affects message reliability, as they do not reflect the reality. This could be performed by manipulating in-vehicle sensors, or by altering the sent information. Imagine that a vehicle reports an accident in road E-7, while it really took place in E-9. Such information should compromise such messages´ trust. Even worse, sending **false warnings** (e.g. the accident didn´t take place) would also affect the whole system reliability. In this way, mechanisms to protect against such inappropriate data should be put in practice in vehicular contexts.

REVIEW OF SECURITY PROPOSALS OVER VANETS

In recent years, there have been a plethora of contributions related to VANET security. All those previous works are based on different techniques to achieve their security goals and so to protect VANETs against the described attacks. In this Section we will analyze the main existing proposals to provide the security services in VANETs. In this way, the reader will discover the most relevant trends and the most used cryptographic tools for each security requirement. Although availability issues have to be considered while designing all mechanisms, some specific mechanisms have also been described here. Each subsection will focus on a different security requirement.

Identification mechanisms

Vehicular contexts have an interesting feature related to identity management. As opposed to classical computer networks, in which no central registration exists, vehicles are uniquely identified from the beginning. Indeed, this process is performed by both manufacturers and the legal authority. Manufacturers assign each vehicle a Vehicle Identification Number (**VIN**). On the other hand, legal authorities require vehicles to have a **license plate**. Both identifiers are different by nature. Whereas VINs are intended to uniquely identify manufactured vehicles, license plates are assigned to every vehicle registered in an administrative domain. Thus, VINs cannot be changed for a given vehicle, whereas license plates can change over time (NZ Transport Corporation, 2006). Moreover, license plates are intended to be externally visible. This issue has an immediate consequence related to privacy preservation - vehicles are not completely anonymous, as visible tracking is currently possible (Parno & Perrig, 2005).

Authentication and privacy issues

With respect to electronic identification, Hubaux *et al.* have proposed a natural extension of license plates called **Electronic License Plate** (ELP) (Hubaux & Capkun, 2004). This credential is issued by the legal authority, allowing vehicles not only to get identified, but also to authenticate themselves. However, as this credential includes the vehicle´s real identity, it makes possible to track a vehicle. Thus, it is necessary to design a mechanism that balances authentication and privacy.

Public key certificates are envisioned for this purpose. These are electronic documents that link a public key with a subject´s identity. However, using real or permanent identity would allow tracking. As opposed from that, these credentials should not make the vehicle to be completely anonymous. Liability attribution is required by the legal authority whenever misbehavior (e.g. traffic offence, false warning) is detected. This tradeoff is called **resolvable anonymity**. Two different mechanisms have been proposed to satisfy this need in VANETs – **identity-based cryptography** and **pseudonymous short-lived public key certificates.** Although they are based on different cryptographic techniques, their underlying processes of creation and use are similar. We will focus on certificates as it is the mechanism proposed in the

security standard in the area, IEEE 1609.2 (IEEE Computer Society, 2006). Particularly, *pseudonymous certificates* allow providing both authentication and privacy protection (Callandriello, G. Papadimitratos, Lloy, & Hubaux, 2007). Readers interested on identity-based cryptographic mechanisms can refer to (Sun, Zhang, & Fang, 2007).

In the following subsections we will describe these certificate´s creation, use and revocation. In the last subsection, other privacy preserving techniques not related with authentication will be explained.

Creation of pseudonymous certificates

Pseudonymous certificates must be issued by a trusted authority. A **Vehicular Public Key Infrastructure** (VPKI) is often assumed for this purpose (Raya, Papadimitratos, & Hubaux, 2006). Figure 3 shows its composition and its relationships with other entities that were introduced on the VANET model.

VPKI is composed by a set of Trusted Third Parties (TTPs) in charge of managing pseudonymous certificates. It is assumed to be structured hierarchically. There is a single root Certificate Authority (CA) in each administrative domain (e.g. a country) and a delegated CA in each region within that domain. As vehicles from different regions (or even domains) can encounter themselves in a VANET, it is generally assumed that these CAs will be mutually recognized.

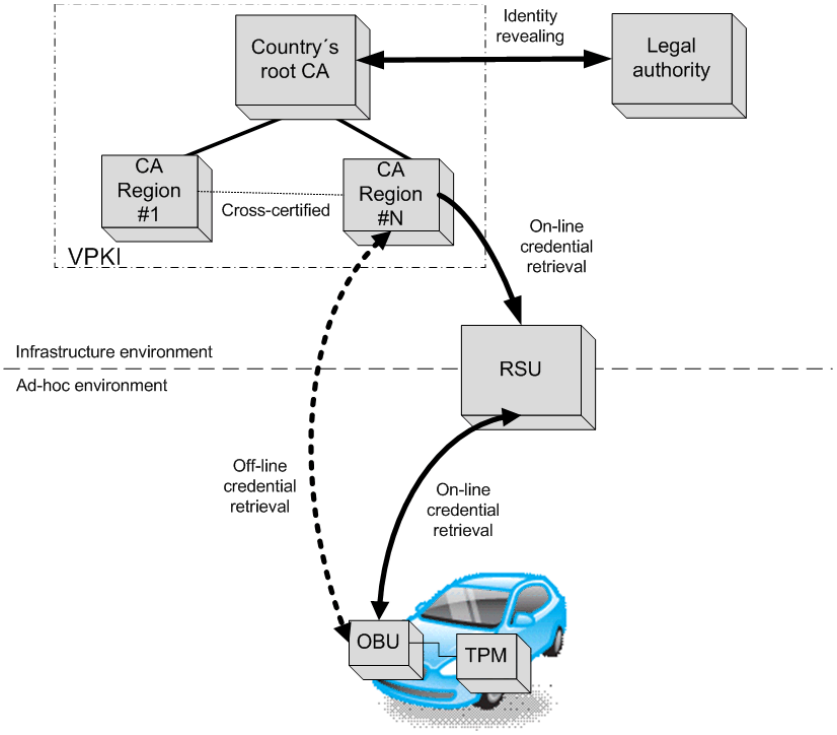

Figure 3. Alternatives to retrieve vehicular credentials

Taking the need of resolvable anonymity into account, there must be a relationship between the vehicle´s real identity and each of its pseudonyms. In fact, as reports are issued to people (and not to vehicles), there are two different steps to link the pseudonym with the vehicle owner´s real identity. The relationship between ELP and pseudonym is managed by the VPKI, whereas the link between ELP and the owner´s identity is only known by the legal authority. Once misbehavior is detected, the authority will contact VPKI in order to get the ELP related to a specific pseudonym. As this identity resolution removes the privacy protection, this process has to be performed only when necessary.

Credentials must be created and stored in the vehicle before using them. It involves creating the pseudonym and the associated keying material, and afterwards performing the

certification process by the corresponding CA. Although the second part can also be performed by the TTP, there are two different proposals related to pseudonym and keying material generation. A straightforward solution is to let the CA create all that information. In this case, all certificates could be created offline and sent to the vehicle periodically (e.g. in the periodic inspection). However, this requires a high amount of storage in the vehicle. Moreover, as they are short-lived, not having enough certificates would lead to a privacy problem. To solve this matter, other proposals let the vehicle create all that information when required. In this way, they contact VPKI through deployed RSUs and send the created pseudonym and public key. VPKI sends in return the credential built. This second proposal is enabled by vehicle´s TPMs, which have a reliable storage and cryptographic processing. An inherent advantage of this method is that the private key associated with the pseudonym never leaves the TPM, so higher security is achieved.

Use of pseudonymous certificates

To harden tracking, each credential should not be used for a long time. Thus, a change policy should be established. Nevertheless, the process of **pseudonym change** is far from trivial. Its effectiveness is directly related to how difficult would be for an attacker to link both pseudonyms (i.e. the former and the new pseudonyms). **Mix contexts** have been proposed to perform such changes (Gerlach, 2006). These areas are unmonitored by any RSU and are preferably put in road intersections. All communications are stopped while being inside that area. Vehicles may change their pseudonyms before leaving it. In this way, when many vehicles enter on this area, their new pseudonym is difficult to guess when they left the mix context.

On the other hand, even if a secure pseudonym change were employed, it would not be enough to achieve a complete privacy protection. Recall that VANETs, as any other protocol network architecture, involves different identifiers in each of the considered levels (e.g. MAC, IP, etc.). In this way, it is necessary to change them all at the same time to avoid traceability (Papadimitratos, et al., 2008). However, some physical features of communication devices could make them identifiable, despite these changes of identifiers. For example, radio-frequency fingerprinting enables a receiver to identify the source. (Kargl, et al., 2008)

Revocation issues of pseudonymous certificates

The use of public key certificates requires managing their different status. Apart from issuing them, sometimes it is necessary to revoke them. For example, if a vehicle starts sending false information, revocation must be performed to reflect this matter. In the same way, if a RSU is compromised, its certificates should be revoked as well. In this way, the remaining entities will be able to identify those with a bad or incorrect behavior. However, distributing and updating such revocation information to all vehicles raises a challenge. If there are no more communication media than the own VANET, no TTPs (like the corresponding CA) can be assumed to be permanently available. Thus, Online Certificate Status Protocol (OCSP) or, in general, any online solution is not suitable for this context.

Several **Certificate Revocation Lists** (CRLs) distribution protocols have been proposed for this purpose. As VANETs can have a great amount of nodes (i.e. vehicles), so CRLs could be heavy. To distribute these lists efficiently, Revocation using Compressed CRLs (**RC^{2}RL**) has been proposed (Raya, Papadimitratos, Aad, Jungels, & Hubaux, 2007). It divides the CRL into several self-verifiable parts. Moreover, CRL´s size is strongly reduced by using Bloom filters. Bloom filters are designed to know probabilistically if something (a key identification number, in this case) is contained within a set (the group of revoked keys). Applying such filters to CRLs allow them to be so light that can be delivered even through Radio Data Systems (RDS). Research results over this protocol have shown that it is possible to get a whole CRL (of 200 KB) in around ten minutes, having a RSU every kilometer (Papadimitratos, Mezzour, & Hubaux, 2008).

Other privacy-specific issues

Although the proposed authentication techniques respect the *unlinkability* and *untraceability* principles, privacy must also be considered in data sharing. In particular, location information can be employed to trace a vehicle, even if pseudonyms are in use. It is necessary to offer the minimum required information to other vehicles, while keeping it useful. **Location cloaking techniques** have been proposed to satisfy this tradeoff (Hoh, Gruteser, Xiong, & Alrabady, 2007). In this way, location information is only offered when enough protection is achieved, that is, when the attacker is so confused that the probability of tracking is below than a threshold. **Aggregation** is also considered for this purpose, which allows sending only aggregated data, thus minimizing the amount of private data sent (Duri, et al., 2002).

Non-repudiation

Non-repudiation aims to avoid one entity to deny having done some action. The most common examples in computer networks are related to sending some information (NRO, **Non-repudiation of Origin**) or receiving it (NRR, **Non-repudiation of Receipt**). However, both services are different by nature and so are their implementing mechanisms in VANETs. Indeed, while NRO has been extensively considered in VANETs, NRR has received less attention. The following subsections explain each of them separately.

Non-repudiation of origin

NRO is traditionally implemented in VANETs using **digital signatures**. In this way, the sender signs all the information to be sent, allowing the receiver to have a proof of this action. The receiver can verify this signature using the public key of the sender. **Elliptic Curves Cryptography** (ECC) is envisioned as the best solution because of its high performance. In fact, IEEE 1609.2 standard, which covers security in VANETs, establishes ECC mechanisms to be employed in vehicular communications (IEEE Computer Society, 2006). **Group signatures** (e.g. Boneh *et al.*, (Boneh & Shacham, 2004)), which are a specific type of digital signatures, have been proposed in this field. It allows each group member signing without revealing their identity to the signature verifier. Only a TTP (in the vehicular context, the legal authority) could reveal the real identity of the signer. As this solution deals with non-repudiation while preserving privacy, it has been widely used.

Two steps are required to perform a complete validation of a signature, each presenting a different difficulty level from the VANET point of view:

- **Signature checking**. This requires applying the public key to the received message and comparing the resulting value with the calculated hash value of the information. If both values are equal, then the signature is correctly calculated. As vehicles are assumed to have enough computational resources, all these operations are feasible in this context. Nevertheless, as availability is required, faster mechanisms are preferred.
- **Certificate(s) validation.** It is necessary to validate the public key certificate of the signer, and all those contained in the certification chain (e.g. Root CA´s certificate, regional CA´s one). This consists of verifying that it is not outdated, that its own signature is correctly calculated, and that they are not revoked (i.e. contained in the CRL). If all these checks are successful, they are considered as valid. However, distributing such revocation information is far from trivial, as it was explained in the "Authentication" section.

Non-repudiation of receipt

NRR, on the other hand, has not been extensively explored in VANETs. This service will be highly relevant in the future, where notifications and other liability-related messages will be received by vehicles. For example, if dynamic speed limits are in place, they will be sent to all passing vehicles. In this situation, there should be a proof to attest that the vehicle received such information. Otherwise, speeding fines can be unfair, as the vehicle should claim not

having received such information. A group-based solution like the one proposed in (Sampigethava, Huang, Li, Poovendran, Matsuura, & Sezaki, 2006) is useful to achieve this goal. In that scenario, the **group leader** is used as a **delivery party**. It acts as a proxy between RSUs and the group members. However, this approach has some important drawbacks. Firstly, the problem is only reduced to a NRR problem between the group leader and the receiving member. Note that existing protocols to solve this problem require several data interchanges or having an inline/online TTP, so their suitability in this context should be carefully analyzed (Kremer, Markowitch, & Zhou, 2002). Secondly, group members are often volatile, so this would be preferable for permanent groups, that is, those composed by non-volatile members (e.g. cars of an enterprise). Thirdly, using a regular vehicle as a proxy could compromise its availability. Having a big group (i.e. tens of vehicles) would imply a great amount of messages to deliver, so scalability problems could appear. And finally, the NRR proof would be stored into the leader. As these proofs would be needed by the legal authority, they should be securely collected from them. Moreover, this collection should be as continuous as possible, as the leader vehicle could get out of range or even have some functioning trouble (hardware fault or even a crash).

Confidentiality

As it was introduced on Section "Security requirements for VANETs", confidentiality in VANETs is needed in V2V group communication. Regarding to group communications**, three main proposals** have been made so far. They are different in nature and purpose and so are their security mechanisms. The first one involves **RSUs to control a region** (Verma & Huang, 2009). Vehicles entering that region should register within that RSU. Once this registration –which involves mutual authentication – has been performed, the RSU sends to the vehicle a symmetric key. This key is shared with all vehicles in that region for a period of time, and it´s used to encrypt those vehicle´s communications with others in that region. In this way, the group is formed by those vehicles in a region at a specific time. Depending on the RSU´s range, this group would be too big and perhaps confidential communication would be useless. A way for alleviating this problem is to divide a RSU´s region into small parts, called 'splits'. Now, all vehicles in that split become a communication group. Moreover, the next split´s key can be calculated individually by vehicles. In fact, once a vehicle is passing to the next split, it can employ their respective keys. These vehicles (called *gateways*) can perform inter-group communication. In this way, only one registration process is still needed in each RSU. A variant of this should be employed to create groups of stakeholders, like all potential clients approaching a supermarket. In this scenario, key management should be performed by the service provider (in the previous example, the supermarket).

The second proposal for group communications is based on establishing **self-organizing geographical regions** (Raya, Aziz, & Hubaux, 2006). A vehicle becomes a member of a group depending on its location. Furthermore, a group leader is needed. This election is performed automatically (e.g. the most centered vehicle). The leader is in charge of creating and delivering the symmetric key. As opposed to the previous proposal, this option allows a group to have a longer communication period (i.e. it is not constrained by the range of the RSU).

The last trend to perform group communication is based on **Attribute-Based Encryption** (ABE) (Hong, Huang, Gerla, & Cao, 2008). Each vehicle has a set of attributes (e.g. kind of vehicle, name of its company, etc.). Once manufactured, credentials for those attributes are inserted in the vehicle. Each attribute is associated with a single public key. However, its private key is divided into several parts, called *key shares*. Each key share is installed in a different vehicle. In this way, only members of that group will be able to decrypt sent messages. This proposal has been extended to allow dynamic attributes. For example, a message of a taxi company is only addressed to those taxis that are near the airport. RSUs (or other alternative communication means) should be employed to deliver the key shares related to these dynamic attributes.

Availability. DoS and uncollaborative behavior prevention

Although availability must be taken into account in the remaining security mechanisms, some specific threats must be faced as well. In particular, a node´s selfish behavior could affect the overall network performance. For example, if a node does not take part in routing algorithms or if it overloads the communication channel with spurious requests, the VANET performance is lowered. Using **incentives** have been proposed to deal with this issue. For example, **Nuglets** are an electronic currency which is got when nodes participate correctly in networking issues (Buttyan & Hubaux, 2001). In fact, to prevent selfishness, several applications require having an initial Nuglet balance to participate in.

Information trust

Traditionally, information trust has been established by means of entity trust. In other words, the more reliable an entity was, the more credible its messages were. However, in this distributed context, entity reputation is not easily reachable. A vehicle can encounter with one another for a short period of time, and perhaps they will never find them again. For this reason, it is the information itself which has to show its truthfulness. This has been called as **situation aware trust**, that is, the current situation must allow evaluating the data trust (Hong, Huang, Gerla, & Cao, 2008).

Every vehicle has to check the reliability of the received messages. Apart from checking the used cryptographic values (if any), it has to evaluate if the contained information could be true. For this purpose, **plausibility checks** have been proposed. In such mechanism, vehicles examine every message based on their previous knowledge. For example, if a vehicle receives a report alerting for road congestion, but its sensors does not reflect any other vehicle around, the message trust could be lowered. For managing such trust, artificial intelligence techniques like neural networks can be employed (Lo & Tsai, 2007).

Nevertheless, this comparison is made only against the own knowledge. It is also useful to compare the message data against the perceptions of other vehicles. Raya *et al.* have proposed a framework for this purpose (Raya, Papadimitratos, Gligor, & Hubaux, 2008). In their work, they propose establishing a measure of trust for each message sent by other vehicles. This measure is based on some static factors (e.g. which kind of vehicle reported the event) and some dynamic ones (e.g. the proximity of the reporter to the event). Moreover, messages from different entities referring to the same event are grouped – trust is then assigned for *events*, not only for messages. The **event credibility** has to be calculated in real-time. Different calculation procedures have been proposed, each one based on different assumptions:

- **Two directions reporting**. Only events that have been reported by two vehicles driving in opposite direction will be considered (Park & Zou, 2008). This method takes advantage of the own nature of roads (where cars can drive in both ways in highways). Moreover, it would be harder for an attacker to compromise both driving directions. However, this could be only applied where such roads exist.
- **Threshold-based trust**. An event is considered trustworthy when it has been endorsed by t different vehicles (Daza, Domingo-Ferrer, Sebé, & Viejo, 2008). Although it would be better to establish this limit dynamically, it is currently unclear how to deal with this issue. Moreover, if pseudonyms are employed, it would be impossible to assure that all endorsing vehicles are different. **Message Linkable Group Signatures** (MLGS) have been designed for this purpose (Domingo-Ferrer & Wu, 2009). They allow verifying this issue while respecting the endorsing vehicles´ anonymity.

There is another technique that, although not related with improving data trust, could negatively affect this security requirement. Aggregation techniques have been proposed for improving the overall efficiency of data interchange. In this way, messages are grouped by a node and only the result is sent. This aggregation can be performed syntactically or semantically. However, a malicious node could perform an **invalid aggregation**, so information trust could be compromised. To alleviate this problem, it should be useful to **request the aggregator** to provide a proof of his behavior (Picconi, Ravi, Gruteser, & Iftode, 2006). For example, the receiver could challenge the aggregator, requesting to get one of the original

disaggregated registers at random. However, as vehicles are constantly moving, a connection between both cars to perform such challenge could not exist. For solving this, TPMs could be used instead. In this way, the TPM could act as the challenger, requesting the aggregation application to add such register along with the aggregated information. Receivers will be able to verify the validity of the register, as well as to check if it is in accord with the aggregated data. This is a probabilistic validation, as only one (or a small part) of the registers is requested.

CONCLUSIONS. FUTURE RESEARCH DIRECTIONS

Nowadays, vehicular networks are being developed and improved. Several new applications are enabled by this new kind of communication network. However, as those applications have impact in road traffic safety, strong security requirements must be achieved. New mechanisms have to be developed to deal with the inherent features of these networks (extreme node´s speed, decentralized infrastructure, etc.). In this chapter, we have presented an overview of the current security issues over VANETs, focusing on road safety communications. We have introduced a common underlying model for this kind of network, along with its main settings. Furthermore, we have identified the security requirements that are present on each VANET setting. We have shown that, apart from typical security needs (e.g. confidentiality), there are other context-specific ones (e.g. trust assurance over reported data). We have also identified several attacks that can be performed in these networks. Finally, we have described and analyzed the main proposed mechanisms to achieve the security goals.

VANET security is an emerging area in which several future research lines can be pointed out. Although several mechanisms have been proposed, some issues still have to be addressed (e.g. privacy problems due to radio frequency fingerprinting). Moreover, as different VANET protocols, mechanisms and applications are based on different architectures and assumptions, a common evaluation framework is needed to compare different security research contributions. Simulation results are often offered to evaluate current proposals. However, a common scenario to evaluate alternatives does not exist. Finally, hardware implementation of efficient cryptographic primitives is required in vehicles. In this way, achieving computation availability would be eased.

ACKNOWLEDGEMENT

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

REFERENCES

- Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., et al. (2006). Attacks on Inter-Vehicle Communication Systems - An Analysis. *International Workshop on Intelligent Transportation.* Hamburg, Germany: IEEE Communications Society.

- Armstrong Consulting Inc. (n.d.). *Dedicated Short Range Communications (DSRC) Home*. Retrieved October 2009, from http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

- Boneh, D., & Shacham, H. (2004). Group signatures with verifier-local revocation. *Computer and Communications Security* (pp. 168-177). New York, NY, USA: ACM.

- Buttyan, L., & Hubaux, J.-P. (2001). *Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks.* Laussane: Swiss Federal Institute of Technology.

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

- Daza, V., Domingo-Ferrer, J., Sebé, F., & Viejo, A. (2008). Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology* , 1876-1886.

- Domingo-Ferrer, J., & Wu, Q. (2009). Safety and privacy in vehicular communications. *Lecture Notes in Computer Science* , 173-189.

- Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M., et al. (2002). Framework for security and privacy in automotive telematics. *International Workshop on Mobile Commerce* (pp. 25-32). Atlanta, Georgia, USA: ACM.

- eSafetySupport. (2007). *eCall Toolbox*. Retrieved October 13, 2009, from http://www.esafetysupport.org/en/ecall_toolbox/

- Gerlach, M. (2006). Assessing and Improving Privacy in VANETs. *Workshop on Embedded Security in Cars (ESCAR).*

- Gerlach, M. (2005). VaNeSe - An approach to VANET security. *V2VCOM.*

- Hoh, B., Gruteser, M., Xiong, H., & Alrabady, A. (2007). Preserving privacy in gps traces via uncertainty-aware path cloaking. *Conference on Computer and communications security* (pp. 161-171). ACM.

- Hong, X., Huang, D., Gerla, M., & Cao, Z. (2008). SAT: situation-aware trust architecture for vehicular networks. *Mobility In The Evolving Internet Architecture* (pp. 31-36). Seattle, WA, USA: ACM.

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

- IEEE Computer Society. (2006). *IEEE Trial-Use Std. for Wireless Access in Vehicular Environments.Security Services for Applications and Management Messages (1609.2).*

- Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications Magazine , 46* (11), 110-118.

- Kremer, S., Markowitch, O., & Zhou, J. (2002). An Intensive Survey of Non-Repudiation Protocols. *Computer communications , 25* (17).

- Laberteaux, K. P., Haas, J. J., & Hu, Y.-C. (2008). Security Certificate Revocation List Distribution for VANET. *International Conference on Mobile Computing and Networking* (pp. 88-89). ACM.

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

- Lo, N., & Tsai, H. (2007). Illusion attack on VANET applications - A message plausibility problem. *Globecom Workshops* (pp. 1-8). Washinton D.C.: IEEE.

- NZ Transport Corporation. (2006, July). *VINs: Vehicle Identification Numbers*. Retrieved October 2009, from http://www.ltsa.govt.nz/factsheets/06.html

- Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., et al. (2008). Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communication Magazine* .

- Papadimitratos, P., Buttyan, L., Hubaux, J.-P., Kargl, F., Kung, A., & Raya, M. (2007). Architecture for Secure and Private Vehicular Communications. *7th International Conference on ITS*, (pp. 1-6).

- Papadimitratos, P., Gligor, V., & Hubaux, J.-P. (2006). Securing Vehicular Communications - Assumptions, Requirements, and Principles. *Workshop on Embedded Security in Cars (ESCAR)*, (pp. 5-14). Berlin, Germany.

- Papadimitratos, P., Mezzour, G., & Hubaux, J.-P. (2008). Certificate revocation list distribution in vehicular communication systems. *International workshop on VehiculAr Inter-NETworking* (pp. 86-87). ACM.

- Park, S., & Zou, C. (2008). Reliable Traffic Information Propagation in Vehicular ad-hoc networks. *Sarnoff Symposium* (pp. 1-6). IEEE Communications Society.

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

- Picconi, F., Ravi, N., Gruteser, M., & Iftode, L. (2006). Probabilistic validation of aggregated data in vehicular ad-hoc networks. *International Workshop on Vehicular Ad-hoc Networks* (pp. 76-85). ACM.

- Raya, M., Aziz, A., & Hubaux, J.-P. (2006). Efficient secure aggregation in VANETs. *International Conference on Mobile Computing and Networking* (pp. 67-75). Los Angeles, CA, USA: ACM.

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

- Raya, M., Papadimitratos, P., Aad, I., Jungels, D., & Hubaux, J.-P. (2007). Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks , 25* (8), 1557-1568.

- Raya, M., Papadimitratos, P., Gligor, V., & Hubaux, J.-P. (2008). On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. *Infocom.* Phoenix, AZ, USA: IEEE Communications Society.

- Sampigethava, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2006). CARAVAN: Providing Location Privacy for VANET. *International workshop on Vehicular ad hoc networks.* ACM.

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

- Verma, M., & Huang, D. (2009). SeGCom: Secure Group Communication in VANETs. *IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 1-5). Las Vegas, NY, USA: IEEE.

KEY TERMS & DEFINITIONS

- ABE (Attribute-Based Encryption): Encryption scheme in which only entities having some attributes (e.g. enterprise membership, current location) are able to decrypt the ciphered data.
- DSRC (Dedicated Short-Range Communications): Standard for vehicular communications. It is a variant of the wireless communication standard and it has been called IEEE 802.11p.
- ELP (Electronic License Plate): Electronic credential issued by the legal authority to each vehicle registered within that administrative domain. It is the electronic equivalent to traditional license plates.
- OBU (On-Board Unit): Communication device mounted on vehicles. It allows DSRC communications with other OBUs or RSUs.
- RSU (Road-Side Unit): DSRC communication unit that is located aside the roads. It serves as a gateway between OBUs and the communications infrastructure.
- TPM (Trusted Platform Module): Computing component mounted on vehicles useful for security purposes. It is assumed to be tamper-resistant. It usually offers secure storage, cryptographic processing and a reliable internal clock. It is also called Hardware Security Module (HSM).
- VIN (Vehicular Identification Number): Number assigned by manufacturers to each vehicle. It has a standardized form, so each manufactured vehicle has a unique VIN value.