Full paper: Witness-based evidence generation in Vehicular Ad-Hoc Networks

J. M. de Fuentes, A. I. González-Tablas, A. Ribagorda
IT Security Group, Computer Science Department, University Carlos III of Madrid (Spain)
e-mail: {jfuentes, aigonzal, arturo}@inf.uc3m.es

***Abstract*—Vehicular ad-hoc networks (VANETs) are a novel communication scenario. They allow vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. New services are envisioned through these networks affecting road traffic safety. Current proposals are based on sharing each vehicle´s perceptions about their own environment. Nevertheless, it is also possible for a vehicle to know the status of their neighbours in a given moment. Thus, a vehicle can obtain from their neighbours their perceptions about its status. Neighbours then become witnesses. Sometimes it is necessary to prove a vehicle´s behavior in a given moment (e.g. accident dispute, speeding fines, etc.). As own sensors can be tampered with, having testimonies from witnesses can contribute to have a reliable source of information. In this work we present EVIGEN, a protocol to obtain such testimonies and generate digital evidences. A security analysis is performed to verify the accomplishment of evidence generation requirements.**

***Index Terms*—EVIGEN, digital evidence, VANET, witness.**

I. Introduction

Nowadays, road transport is an essential activity in human daily routine. Because of that, increasing investments are being made, leading to remarkable improvements on this area. On one hand, traffic casualties are lowering each year and countries like Sweden have put the goal of zero road traffic fatalities and serious injuries by 2020 [1]. On the other hand, infotainment is also demanded by passengers to improve their comfort. Thus, it is necessary to have content distribution (DAB/DVB) and also mail and IM access, among others

Information technologies are being strongly improved to deal with such new needs in vehicular environments. Apart from traditional communication technologies (Wi-Fi, GSM/GPRS, etc.), Vehicular Ad-hoc NETworks (VANETs) are being developed as a new means of communication. These networks enable not only Vehicle-to-Infrastructure (V2I, I2V) communications, but also Vehicle-to-Vehicle (V2V) interconnection.

VANETs enable new applications for a better traffic management. It is now possible for vehicles to announce some road hazard, an accident or even a traffic jam. Moreover, special vehicles (firemen patrols, ambulances, police patrols) can announce their presence, making easier for themselves to have a free way. These applications are mainly based on sensors currently incorporated into vehicles. Vehicles now share their own vision of their environment based on their sensor measurements. In this way, drivers can have an enhanced vision of the current status of the road.

The current state-of-the-art technologies enable a new family of applications through VANETs. In particular, there are situations in which it is necessary for a vehicle to proof its recent behavior. For example, when an accident happens, it is useful to have an accurate description of the situation for liability purposes. As this description would be employed in courts, a digital evidence containing such data must be built. Although it is often assumed that vehicles will be equipped with reliable components (e.g. TPMs, EDRs), sensors (or the underlying automotive bus systems) can be tampered with. Although countermeasures have been proposed, they are not present on all current buses [2]. For this reason, own sensor measurements should not be employed for building such evidences, or at least it should be advisable to have an alternative approach.

A more reliable data source about a vehicle´s behavior is needed. VANETs can be useful for this purpose. Indeed, vehicles driving around one another could act as its witnesses. Previous contributions have shown the chance of a vehicle to relate some of its sensor measurements with the originating vehicle [3]. These data can be now shared by using inter-vehicle communications in VANETs. Taking these external data into account, creating a false description of the situation will be harder, as the attacker should control the majority of witnesses.

In this work we propose EVIGEN (EVIdence GENeration) protocol for obtaining such data about one´s behavior from nearby vehicles. The protocol also involves the creation of a digital evidence, that is, a digital document to attest the collected data. This evidence will be useful for supporting a hypothesis when contradictory versions are offered in a dispute resolution. Concretely, the following applications are envisioned to be addressed by EVIGEN:

1) Spatial-temporal attestation. To show that a vehicle was in some place at a given moment.
2) Adequate behavior. A vehicle´s speed was under the maximum limit whenever a speeding fine was issued.
3) Accident reconstruction. To have a record of the last actions performed by a vehicle when an accident happened.

An interesting feature of EVIGEN is that it allows building a unified evidence, taking into account the received data. This will be preferred in courts, where proofs are expected to be as specific as possible while being useful for the process. For this purpose, each witness will send an authorization token along

with their estimations. It will allow the requester to reflect each witness´ endorsement to the unified value.

For assuring the security properties of the data at stake, the protocol makes use of the security tools proposed by the current standard on this area (IEEE 1609.2 [4]). To evaluate the security of the proposal an analysis is performed, including privacy issues.

Paper outline. On Section II the term evidence is clarified and the requirements for obtaining such evidences are presented. The underlying model of EVIGEN is introduced in Section III. The proposed protocol is presented in Section IV, while in Section V the corresponding verification process is described. The security analysis of the proposal is performed on Section VI. Some practical issues related to EVIGEN will be presented on Section VII. The related work is presented on VIII and Section IX shows the lessons learned from this work and future research lines.

II. Digital evidences. Creation in vehicular environments

In this Section we present a definition of digital evidence. Once its main features have been introduced, we will elaborate on which tools can be useful to get such evidences on a vehicular environment.

A. Evidences and digital evidences. Definition and requirements

The term *evidence* has been widely addressed so far. Initially, evidence may be defined as "any material which would aid the court in establishing the probability of past events into which it must inquire" [5]. This definition is very general and does not reflect the own nature of computer-based evidence. For this purpose, the International Organization on Computer Evidence (IOCE) defined *digital evidence* as "the information stored or transmitted in binary form that may be relied upon in court" [6].

Taking into account these definitions, we speak about digital evidences when the conclusions that can be derived from it are indisputable. Nevertheless, although digital evidences are expected to be probative, in many legal systems it is the judge who has to consider their relevance within a process. This decision is mainly based on the general principles of *admissibility*, which are not the same in all countries. However, the admissibility is generally linked to some basic requirements [7]:

- Authenticity and reliability. The proof must be unaltered and must contain reliable data.
- Completeness. The proof must contain as much data as possible to describe the fact.
- Law compliance. It is especially relevant that the proof has not been obtained by violating other rights.

B. Tools for building digital evidences in vehicular environments

The creation of digital evidences requires an extremely strict and secure process. This is not easily reachable in vehicular environments, where events happen in an unpredictable manner and there is not a global infrastructure to register them. Reliable data acquisition and recording are current problems in this scenario. Nevertheless, some other inherent features of vehicles can be helpful for this purpose. In the following we will show how VANETs and reliable hardware modules can help creating digital evidences.

The *completeness* principle previously introduced makes essential to collect all the potential information for creating the evidence. Recalling the target applications cited on Section I, the following list illustrates the main pieces of information for each specific use:

- Spatial-temporal attestation: Position, time, identity.
- Correct behavior: Position, time, identity, attribute (e.g. speed).
- Accident reconstruction: Position, time, identity, description of the situation (including: lane, preceding vehicles´ attributes, etc.)

Different sources are commonly employed to obtain these data. Positioning systems (e.g. GPS) or sensors attached to the vehicle (e.g. rain sensors, tyre pressure, etc.) are only two examples. However, these sources could be tampered with. Positioning systems could be attacked in practice (e.g. jamming attacks [8]). On the other hand, current automotive bus networks are not strongly protected and could be maliciously altered. Some countermeasures have been proposed, but they have not been incorporated into all automotive systems so far [2]. Moreover, unexpected sensor errors can take place at any time.

Data contained within digital evidences must be reliable. However, sensor information does not assure such quality. Moreover, in our context, digital evidences will be built by a vehicle to get some benefit (e.g. avoiding a speeding fine). Thus, there is a motivation for altering such sensor information - to build a false description of the real situation to achieve such reward. It would be advisable to have independent sources for these data. Such information redundancy would improve the global data quality, as malicious or faulty information could be detected and discarded. This redundancy can be achieved by using VANETs. As vehicles will be equipped with a sensor set, vehicles surrounding a given one can become such information sources for it. These vehicles will be referred as *witnesses* in the remainder.

Using witnesses enable us to have a more complete and reliable data for building evidences. However, the authenticity requirement for evidence admissibility goes beyond the data quality. Some security guarantees must be provided to protect the whole process of building that evidence. As sensor data will be sent among vehicles, integrity must be provided to assure that no alterations have been made. On the other hand, non-repudiation and origin authentication are necessary for the evidence holder. In this way, it will not be able to deny having built such evidence related to itself. Moreover, confidentiality and privacy must be assured for all participants, as sensitive information could be interchanged. Cryptographic tools could be employed for fulfilling all these requirements.

Finally, it is necessary to have a secure storage for the built evidence. Both features (cryptographic processing and

secure storage), along with reliable timestamping, can be performed by Hardware Security Modules (HSM) or Tamper Proof Devices (TPD) [9].

To sum up, in this Section we have shown how nearby vehicles and HSM devices can be employed to build digital evidences. Nevertheless, a communication protocol between the evidence requester and witnesses is still needed. EVIGEN will be presented in the following Sections for this purpose.

III. Model

In this Section we will introduce the underlying model of EVIGEN. For the sake of simplicity, this model has been divided into three main blocks: network model, vehicular model and threat model. The next sections present each one separately.

A. Network model

The proposed protocol is expected to work on a typical road environment. This is depicted on Figure 1. Although EVIGEN will be more useful in dense networks, only two vehicles are enough to run the protocol. With respect to communication capabilities, each vehicle is assumed to be equipped with an On-Board Unit (OBU). Although they will not be directly employed in our proposal, Road-Side Units (RSU) have been also included in this model. They will be employed for performing some auxiliary tasks, like Certificate Revocation Lists update. Thus, ad-hoc networks will be established between OBUs and RSUs.

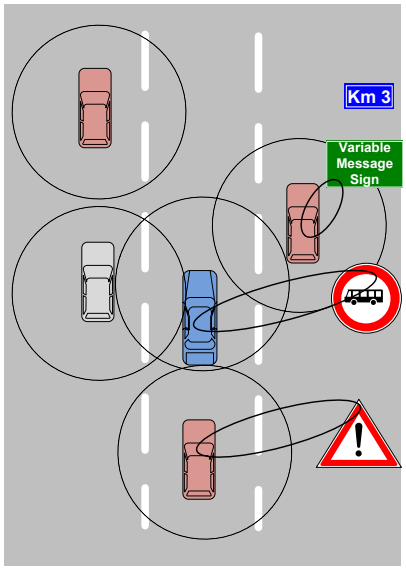

Fig. 1. Expected EVIGEN road model

Note that a global communications infrastructure is not assumed nor necessary for EVIGEN. This assumption makes the protocol more suitable for vehicular environments. However, it constraints some classical solutions in data security, such as those based on online Trusted Third Parties (TTP) like Certification or Timestamping Authorities. Nevertheless, we assume that a Public Key Infrastructure (PKI) exists, as it is specified in the main information security standard on this area (IEEE 1609.2, [4]).

B. Vehicular model

Every participant vehicle is assumed to be equipped with a HSM-alike device. This will be useful for timestamping, performing cryptographic operations and storing evidences. With respect to their sensing capabilities, it is assumed that they will have a set of sensor devices. They would range from ultrasound sensors up to video cameras. However, it is necessary for vehicles to link their perceptions to the originating vehicle. This can be achieved by fusion of communication measures and sensor perceptions. For example, if the preceding vehicle is sensed to drive slower than the own vehicle, and there is a message (e.g. beacon) received from a vehicle in front claiming some identity, a link speed-identity can be established. Although this is out of the scope of this paper, fusion techniques are currently being developed for this purpose with promising results [3].

With respect to identity management, every vehicle is assumed to have a long-term identity (e.g. Electronic License Plate). Moreover, for privacy preservation purposes, vehicles can have a set of pseudonyms. Each pseudonym should be related to a certified public/private key pair. To avoid tracking, pseudonyms should be changed frequently (e.g. use of mix contexts [10]). We propose using resolvable pseudonyms such as those proposed in [11].

It is assumed that vehicles will share some traffic data using VANET. These data interchanges can be performed in an independent way, or in a collaborative paradigm. The former can be achieved by periodically sending *beacons*, each one containing information about the sender´s situation and sensed environment. The latter has multiple shapes, such as Cooperative Cruise Control (CCC). Under this paradigm, vehicles are grouped because of their driving parameters (e.g. destination, desired speed, etc.). In this way, a group member has a great knowledge of the remaining members´ context. This information sharing is interesting for the purpose of this work, as they allow vehicles to know better which is the behavior of their surrounding vehicles.

C. Threat model

Any vehicle (both requester and witnesses) can become an attacker to EVIGEN. Nevertheless, we assume that in every protocol execution, there will be a majority of honest witnesses. On the other hand, we assume that attackers are not *colluding*, that is, they operate independently and they do not collaborate in their actions. Under this assumption, attackers cannot claim the same false value. In this way, dishonest (or faulty) testimonies will be easily identified and isolated. Taking into account the main objective of their attacks, different kinds of attacker can be identified:

- *Protocol ineffectiveness*. This attacker sends false information when acting as a witness.
- *Protocol inefficiency.* This attacker does not take part in the protocol, neither as a witness nor as an intermediary vehicle (when needed).

- *Flooding.* This attacker aims to overload the vehicular communications channel. He sends continuously requests for evidence generation.
- *Eavesdropping.* This attacker records all messages related to EVIGEN. He aims to find confidential or private information, such as the location of an entity.

Taking these attackers into account, the security analysis on Section VI will show how EVIGEN is protected against them.

IV. Witness-based digital evidence generation protocol

Taking into account the discussion about digital evidences in vehicular environments (Section II) and the underlying model (Section III), in this Section the proposed protocol is described. A protocol overview is firstly presented. Afterwards, the notation in use is explained and finally the protocol steps are described.

A. Overview

EVIGEN is intended to create digital evidences attesting a vehicle´s behavior or situation in a given moment. This evidence will be presented to an Authority (e.g. a judge) in a dispute resolution process. As discussed above, nearby vehicles can serve as an external and impartial source of information. Thus, there are two different active roles in this protocol: the vehicle which requests the evidence generation ("requester") and those vehicles which can give some data for building it ("witnesses").

The main goal of EVIGEN is to create an evidence based on the received witnesses from adjacent vehicles. Considering the high mobility of vehicles, the protocol must be as lightweight as possible. For this purpose, EVIGEN consists of two communication steps: request of information and testimony collection. These steps are represented on Figure 2.

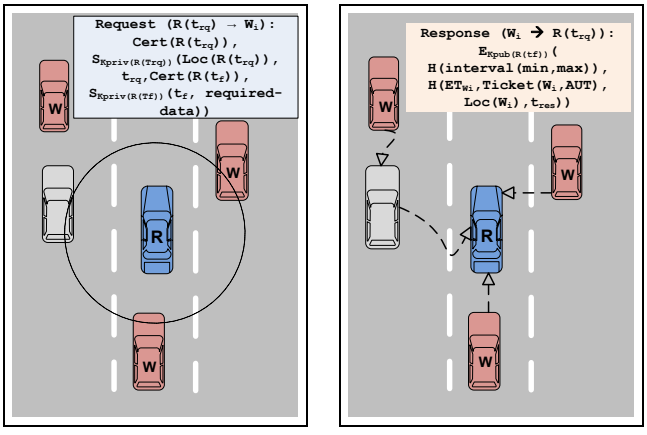

Fig. 2. EVIGEN protocol steps.

In Figure 2, the requester is the blue vehicle (marked with 'R') while red cars (marked with 'W') are potential witnesses. White vehicles are those which are near the requester, but are not able to be witnesses. That could be the situation in which a vehicle has recently arrived near to the requester, but does not know any valuable data about the requester´s behavior in the past. They are, however, indirectly useful for the purpose of EVIGEN - they can serve as proxies between both requester and witnesses. Note that new intermediaries can appear at any moment, because of the own nature of vehicular movements.

Each witness will send its estimation about the requested data. Sensor measurements experience some kind of uncertainty, which have to be reflected in their testimonies. As evidences are intended to be employed in courts, it is preferable to build the description of the situation as simple as possible. In this way, the authority will be able to understand easily the circumstances in which some event happened. This implicit requirement makes preferable to reach a consensus among witnesses. Nevertheless, performing a consensus protocol (e.g. [13]) among witnesses would not always reach a solution within the required time. Thus, they are not suitable for this context. For solving this, the requester in EVIGEN is allowed to build the consensus based on the received testimonies.

Such consensus consists of the value set agreed by most witnesses. Although there would be other ways of establishing such consensus, we argue that it is the most intuitive one. Along with their testimonies, witnesses send a special token called Endorsement Token (ET). It contains the conditions under which the requester is allowed to endorse such a value (i.e. who is the requester and which information can be endorsed on the witness´ behalf). In this way, the requester will not be able to illegally build an evidence using information not allowed by any of the endorsing witnesses.

B. Notation

The following notation will be in use for describing EVIGEN. First of all, existing roles will be noted as:

- R(t), Requester. It denotes its pseudonym on time *t*.
- W_i, Witness *i*. It denotes its pseudonym in use in each protocol execution.
- AUT, the Authority to which the evidence will be sent.

Cryptographic fuctions (selected within those proposed in IEEE 1609.2 [4]), will be marked as follows:

- H(M), hash function over the message 'M'. It denotes the message 'M' and its hash value.
- $E_K(M)/D_K(M)$, asymmetric encryption/decryption over 'M' using key K through ECIES algorithm.
- $SE_K(M)/SD_K(M)$, symmetric encryption/decryption over 'M' using key K through AES-CCM algorithm.
- $S_K(M)$, signature over 'M' using key K through ECDSA algorithm. It denotes the message 'M' and its signature value.
- Verify(S,Cert(X)), verification operation over signed message 'S' using the key in Cert(X) public key certificate.

Finally, data at stake are noted as follows:

- Cert(X), public key certificate of entity (generally a vehicle) X.
- interval(a,b), expression of all values contained in interval [a,b], independently of the nature of *a* and *b*.
- contains(data,min,max), boolean function which determines if data $\in$ interval(min,max).
- t_i, time value of the moment *i*, built by the sender´s HSM.
- Loc(X), current location of entity (generally a vehicle) X.

C. Protocol description

Following the description of EVIGEN is presented. Each of the messages involved is explained, along with the computation needed to build them.

Phase 1. Request of information

In this message, the requester sends a signed message specifying the required data. The time when this request is sent will be noted as t_{rq}. On the other hand, the time the required-data refers to, will be marked as t_f. Recall that the requester´s pseudonym could be different in both moments. Thus, in this message the requester must show who it was at time t_f. This is done by digitally signing with both private keys, as follows:

$R(t_{rq}) \rightarrow W_i$: Cert($R(t_{rq})$),$S_{Kpriv(R(Trq))}$(Loc($R(t_{rq})$),t_{rq}, Cert($R(t_f)$),$S_{Kpriv(R(Tf))}$(t_f, required-data))

The required data depends on the target application of the evidence, as introduced in Section II-B. The message is sent by *geocasting* to all surrounding vehicles in a reasonable range. In this way, channel overload is alleviated. Selected message format is a signed WSM, as specified in IEEE 1609.2 for inter-vehicular sporadic communications [4].

Phase 2. Testimony collection

In this second phase, witnesses send their estimations to the requester. Although this phase requires some time to get finished, for the sake of simplicity we will assume that it is completely performed on the time of the response (t_{res}). This step only takes place if the previous request was valid. Request validation applies not only to its signature, but also to its location and time. In [14], mechanisms for such checks are described. If it was a valid request, this phase is formed by the following steps:

2.a. Data estimation based on external sources.

Each of the witnesses should build their own estimation about the required data. They have probably received some external data related to the requester. For example, previous beacons or overheard Cooperative Cruise Control messages could be seen as external sources of information. Using them, a preliminary interval can be designed:

W_i : beaconing($R(t_f)$) x Coop. Cruise Control($R(t_f)$) ⇒ preliminary_interval

2.b. Plausibility checks.

The composed interval can be analyzed by using the witness´ own knowledge. It is related to its own situation (position, speed, etc. at the requested moment) and the previous measures obtained by its sensors (radar, video, etc.). Taken such data into account, some values of the preliminary interval can be discarded. For example, let´s consider a request referred to the speed. Assume a preliminary_interval of (100,120) mph. If the witness was driving in t_f at 110 mph. and sensors indicate that the requester was overtaken, it would not be possible for the requester to drive faster than 110 mph. Thus, values from interval (110,120) would be discarded.

W_i : preliminary_interval x sensors measurements ⇒ interval(min,max)

Processing tasks involved in this step are complex. Different sources of information must be taken into account, along with their uncertainty. Previous contributions have focused on this area. Raya *et al.* proposed a framework to evaluate the trustworthiness of data reported by other nodes [15]. Moreover, Wex *et al.* review other proposals for trust establishment [16]. For the purpose of EVIGEN, any calculation method that deals with these different sources could be used. Nevertheless, efficiency considerations would be critical, as this operation should be performed as fast as possible.

2.c. Data sending.

If the previous interval contains any value, the response can be sent. This response is encrypted with the receiver´s public key in the time of the requested data (t_f). It consists of three parts:

- Testimony. It contains the witness´ estimation about the required-data (i.e. interval(min,max)). This part is intended to be read by the requester.
- Endorsement Token (ET). Once the responses from all witnesses are collected, a common value for the requested data is seeked among as much witnesses as possible. Then, requester will use this token to reflect the witness´ endorsement to such value. As explained on the protocol overview, this mechanism is intended to build a consensus without requiring a heavy protocol.
  ET_{Wi} = $SE_{Ket(Wi)}$(W_i,$R(t_f)$, interval(min,max),t_f,t_{res})
  ET is, in fact, a ciphertext for the Authority. It contains the endorsement conditions for that witness. The ciphering key is sent inside the following Ticket.
- Ticket. It contains the key $K_{et(Wi)}$ employed for ciphering the ET introduced above. It is based on the classical mechanism of digital enveloping:
  Ticket(W_i,AUT) = $E_{Kpub(AUT)}$(Cert(W_i), $S_{Kpriv(Wi)}$($K_{et(Wi)}$))

Thanks to this data distribution, the witness´ identity is hidden for the requester. This is particularly relevant for those cases in which the testimony is not suitable for the requester´s intentions. In those situations, the requester could take reprisals against the witness.

The whole response is formed as follows. Note that the testimony is sent to $R(t_{rq})$, that is, the requester pseudonym when the first message (request) was sent:

$W_i \rightarrow R(t_{rq})$: $E_{Kpub(R(Tf))}$(H(interval(min,max)),H(ET_{Wi}, Ticket(W_i,AUT),Loc(W_i),t_{res}))

Phase 3. Digital evidence generation.

The requester checks if the received spatial-temporal information is reasonable. He also verifies the integrity of the received testimony. If so, he builds the consensus based on the received responses. As introduced before, if no global consensus exists, the most agreed value (*data*) will be chosen instead. The whole digital evidence (Evid(R)) is built in time t_{evid} using this agreed value and the received ETs. For a number *n* of witnesses, the resulting evidence would be formed as:

Evid($R(t_{evid})$) = Cert($R(t_{evid})$), Evid_info($R(t_{evid})$), where

Evid_info($R(t_{evid})$)= $S_{Kpriv(R(Tevid))}$(data, t_f, t_{evid}), (Ticket(W_1,AUT), ET_{W1}, ..., Ticket(W_n,AUT), ET_{Wn})

This evidence would be finally sent to the Authority:

$R(t_{evid})$ → AUT: Evid($R(t_{evid})$)

V. EVIDENCE VERIFICATION PROCESS

Once the evidence has been created by means of EVIGEN, in this Section the corresponding verification process is presented. The notation in use is the same as presented in IV-B. Except for Phase 1, all phases are executed for each of the endorsing testimonies. Validation is only achieved if all checks are passed.

Phase 1. Signature verification over Evid(R(t_{evid}))

First of all, evidence signature is checked to guarantee integrity and origin:

AUT : Verify(Evid_info(R(t_{evid})),Cert(R(t_{evid})))

Phase 2. Ticket deciphering and endorsement restrictions retrieval

The Ticket is deciphered to obtain $K_{et(Wi)}$, which was used to cipher the Endorsement Token:

AUT : $D_{Kpriv(AUT)}$(Ticket(W_i,AUT)), getting access to (Cert(W_i), $S_{Kpriv(Wi)}$($K_{et(Wi)}$)).

The signature over $K_{et(Wi)}$ is then verified. If successful, symmetric decryption over ET is used to retrieve the endorsement conditions:

AUT : $SD_{Ket(Wi)}$(ET_{Wi}), obtaining (W_i,R(t_f), interval(min,max),t_f,t_{res})

Phase 3. Certificate status verification

Authority verifies if certificates of all involved entities were valid (i.e. not revoked or expired) in the moment they were used (t_{res} for the witness, t_{evid} for the requester)

Phase 4. Endorsement conditions verification

4.a Identity checks

The witness identity must be the same in both Ticket and ET. Moreover, the requester must be the same as that indicated in ET (although it can have changed its pseudonym). Furthermore, the requester and the witness should be different entities. Witnesses should also be all different entities. Finally, the envisioned applications for the digital evidences require the real identity of the requester to be obtained. For performing all these checks, the receiving authority should contact with the entity in charge of managing the pseudonyms.

4.b Legal consensus

Data inside the consensus must be allowed by all witnesses. For this purpose, the function *contains* is employed. Thus, the following expression must hold:

contains(data, min_i, max_i) = true $\forall$ i

4.c Time checks

The time of the evidence data must be equal to that contained in the endorsement conditions. Moreover, t_{evid} must be posterior (but not much) to t_f.

VI. SECURITY ANALYSIS

In this Section, the security analysis of the proposal is performed. The analysis is centered on verifying whether the resulting evidence fulfills the admissibility requirements described on Section II-A. The *completeness* requirement depends on the requester (which has to ask for all necessary data), so the remaining properties, which depend on the security properties of EVIGEN, are analyzed. The first point will deal with the authenticity of the evidence. In the second point, the evidence reliability will be discussed. Thirdly, privacy concerns are analyzed, because privacy is the most prominent right potentially threatened in this context. Finally, other threats will be studied.

A. Evidence authenticity

Evidence authenticity is related to assure that it has not been altered, and that it has been built by some identifiable entities. Moreover, the evidence holder should not be able to deny having issued it. For this purpose, in this Section, entity authentication, non-repudiation and data integrity are discussed. Entity *authentication* matters are partially solved by public key certificates imposed by IEEE 1609.2. However, PKI-based techniques face some problems in decentralized environments such as VANETs. For example, Certificate Revocation Lists (CRL) are not easily distributable to all vehicles. This would allow a vehicle to create evidences based on testimonies whose witnesses use an expired certificate. In such situation, EVIGEN would be useless. Some proposals have been made to deal with this issues, such as the RCCRL protocol, in which Compressed CRL updates are broadcasted by RSUs [17].

Non-repudiation in EVIGEN is assured for the requester of the evidence. The final evidence is digitally signed, so origin and authentication are assured. Non-repudiation of receipt is not required in EVIGEN. Nevertheless, as the generated evidence would be sent to an authority, it will be essential to provide this service in that moment.

On the other hand, *data integrity* is assured in both kind of messages. The request´s integrity is assured by verifying its digital signature. With respect to testimonies, hash functions assure this property.

B. Evidence reliability

Reliability of the evidence data is critical. The use of witnesses (under the assumption of a honest majority) allows EVIGEN to have a more reliable data source. Nevertheless, EVIGEN has two problems (from the requester point of view) which are not yet solved. On one hand, a dishonest witness could offer the requester a different estimation from that included on ET_{Wi}. In this way, the requester could build an evidence which would not fit with such endorsement conditions. On the other hand, different testimonies could be received from the same witness under different pseudonyms. The validation protocol would bring up this issue and would make the evidence less credible.

Both problems are currently present. However, they are assumed to have a limited impact. To put them in practice, it would be necessary to alter the HSM, or to build a different component. Moreover, performing this attack would need to expend some computational power, and no direct benefits are envisioned from it.

Finally, testimonies´ freshness are checked within the verification process. By using HSM´s time source, it is not possible to create *a posteriori* testimonies. Moreover, replay attacks are also useless.

C. Law compliance. Privacy preservation

From a conceptual point of view, the protocol looks for data concerning the recent past behavior of a given vehicle. In other words, surrounding vehicles can establish a link between an identifier (i.e. pseudonym) and its circumstances, and they are able to store that information for a period of time. Moreover, the requester reveals its pseudonym in the past, so traceability is a need in EVIGEN. Indeed, EVIGEN proposes a tradeoff between a privacy loss (traceability) and a benefit (getting a reliable digital evidence). Note that EVIGEN only implies a limited traceability - only nearby vehicles will be able to link two pseudonyms.

Testimonies, on the other hand, are ciphered with the receiver´s public key, so there is no chance of obtaining any information. Intermediary vehicles cannot obtain any private information from testimonies either. With respect to witnesses´ privacy, witnesses´ identity remain hidden for the requester. Furthermore, the witness´ real identity is not revealed in the verification process.

D. Other threats

Availability of the communication capabilities could be compromised if EVIGEN were employed frequently. In fact, every step involves cryptographic operations, so it would be possible (at first) to perform a *Denial of Service* (DoS) attack by flooding of requests (Phase 1). This kind of attack would be especially useful when the evidence is requested for accident reconstruction. In that situation, at least two different vehicles would be affected, so there would be a real interest in avoiding EVIGEN successful execution. This threat is partially alleviated by EVIGEN design - it involves only two communication phases. Moreover, cryptographic functions in use are expected to be efficient. However, this threat should be analyzed in a real environment, where different applications would be running at the same time.

On the other hand, reusing the key K_{et} could be not advisable. That key is employed to cipher the valid endorsement conditions. If it is employed in many messages to the same vehicle, a *clear text attack* could be performed by the requester. This threat is unlikely to happen, but can be easily avoided - it is enough to change the key in each message (or, at least, with a reasonable frequency).

Witnesses offering *false data* will not affect the protocol execution if there is a majority of honest witnesses and dishonest ones are not colluding. This honest majority has been assumed for dense networks, but could not be fulfilled in sparse ones. In any case, the main deterrent should be the legal consequences of such false informations. However, such legal measures are out of the scope of this paper.

Uncollaborative nodes could also be present. It will be always possible for any vehicle to switch off their communication device. This would lead to less witnesses and could make EVIGEN useless. Intermediary vehicles could also avoid relaying messages. To prevent all these undesired behaviors, rewarding protocols for enforcing cooperation could be applied. Previous proposals explained in Buttyán *et al.* could be taken as a basis [12]. The concrete adaptation of such mechanisms is left to future work.

Finally, the use of pseudonyms should not allow to execute *Sybil attacks*. Nevertheless, as pseudonyms are managed by the HSM, it is not possible for a vehicle to use more than one pseudonym at a time, except if the HSM had been compromised.

VII. Implementation issues

The current description of EVIGEN has shown its validity from a theoretical point of view. Nevertheless, some practical issues should be addressed before putting it on a real environment. First of all, EVIGEN requires the vehicles to store *enough* sensor measurements and received data. The storage requirements will be directly influenced by the gap between the time of the event (t_f) and that of the request (t_{req}). Indeed, this gap will be different for each envisioned application. For spatial-temporal attestation, there is no practical upper limit for this gap - a requester would ask the witnesses for its location at a very past moment. Nevertheless, the witnesses´ mobility will bring EVIGEN useless if the required moment is far from the request. The probability of keeping a witness near the requester for a long time diminishes (in theory) with time. Thus, for this application, a reasonable upper limit for the time gap should be established. The second application was to attest the requester adequate behavior in the past. An example is to proof a legal speed when a speeding fine has been notified. In that case, the time gap would be related to the amount of time required to receive the notification of such fine. The last application was obtaining proofs related to an accident. In this case, the time gap is assumed to be short - the request would be sent whenever the accident happens. However, the high difference perceived for each application should be taken into account. A single maximum time gap should be established for all applications.

On the other hand, synchronization is also relevant in this context. Timestamps are assumed to be on both requests and testimonies. HSMs are often assumed to have a reliable time source. However, a secure synchronization method between HSMs would be required. This issue is out of the scope of EVIGEN, but it should be addressed before putting the protocol on practice.

Last but not least, channel overload prevention should be incoporated into EVIGEN. Consider this situation: Once a speeding fine has been received, the affected vehicle asks witnesses for its speed. Once the testimonies have been collected, no valuable consensus is reached (i.e. the most agreed speed value is not useful for the requester´s purposes). In the current version of EVIGEN, it would be possible to repeatedly send requests until a better result is reached. This action would affect negatively the VANET availability, so some mechanism should be added to avoid this situation.

VIII. Related work

The security of vehicular communications has been extensively explored so far [18]. Nevertheless, to the best of our knowledge there are little contributions on evidence generation

in vehicular environments. The most representative contributions are related to accident reconstruction. In [19], HSMs are employed to register all the events produced by the own car. Once the crash has happened, involved vehicles send some beacons to inform the other vehicles. HSM of crashed vehicles is then employed as a *black box*. However, such informations are based on the own vehicle´s sensor measurements, which could be tampered with. Generated evidences validity could be called into question.

On the other hand, [20] performs accident reconstruction by using the own data and the received communications. Nevertheless, data security requirements are not covered in that work. Moreover, they do not provide mechanisms to build a digital evidence.

Evidence generation is also present in the security framework presented by Lin *et al.* [21]. Their focus is on providing security, privacy and efficient traceability. They base their approach in using ID-based cryptography and group signatures. Although the former could be applied directly to our proposal, we have chosen a certificate based solution to be in agreement with IEEE standard.

Finally, group communications could be envisioned as a means to select witnesses. Group formation has been previously studied by Raya *et al.* [22]. Nevertheless, the requester in EVIGEN is requiring information of a moment in the past. Given the volatility of the group formation, it could be possible that current group members were not present at the requested time. For this reason, we argue that this choice would not always be suitable.

IX. Conclusions and future work

In this work we have presented EVIGEN, a protocol for creating evidences about a vehicle´s recent behavior. Data employed for creating such evidence is obtained from the neighboring vehicles, which act as witnesses. In this way, forged sensor measurements from the own vehicle could be used to build the evidence, but no supporting witnesses would be found. EVIGEN allows collecting all testimonies from witnesses, building a unified description of the situation in the required moment. Although each witness sends its particular estimation of the requested value, they also send an authorization token which allows the requester to endorse the agreed value on the witness´ behalf. Moreover, the protocol is executed in two steps, which makes it interesting to be applied in such decentralized and changing environment.

The corresponding verification process has also been described. The security analysis has shown that the requirements for evidence generation are accomplished to a reasonable level. Data obtained from witnesses is adequately protected. However, some security drawbacks have been detected. These problems are related with the witnesses´ dishonest behavior.

Future research work will be centered, in the short term, on solving the detected security problems. Moreover, a simulation-based analysis must be conducted for a practical efficiency evaluation. On the other hand, it would be interesting to incorporate aggregation techniques in EVIGEN. In this way, a witness could offer an aggregated testimony, improving the overall efficiency. However, a detailed analysis is needed in order to address such issue while preserving the security of the information at stake. Finally, a micropayment mechanism will be added to EVIGEN. In this way, witnesses would get a benefit from offering their testimony. Furthermore, only vehicles with enough credit would be allowed to request. Its benefits would be two-fold: it would avoid the requester to overload the channel with requests, and it would encourage witnesses to take part in the protocol.

Acknowledgement

This work is partially supported by Ministerio de Ciencia e Innovacion of Spain, project E-SAVE, under grant TIN2009-13461. Authors want to thank the anonymous reviewers for their valuable comments to improve this work.

References

[1] Whitelegg, J. and Hag, G. Vision zero: *Adopting a target of zero for road traffic fatalities and serious injuries*, Stockholm Environment Institute, 2006.

[2] Wolf, M., Weimerskirch, A. and Paar, C. Security in automotive bus systems. *Proc. 2nd Workshop on Embedded Security in Cars (ESCAR)*, 2004.

[3] Golle, P., Green, D. and Staddon, J. Detecting and correcting malicious data in VANETs, *Proc. of the 1st ACM International Workshop on Vehicular ad hoc networks*, ACM, 2004, pp. 29-37.

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

[5] Murphy, P. *Murphy on evidence* (10th ed.), Oxford University Press, 2007. ISBN: 0199216282, 9780199216284

[6] International Organization of Computer Evidence (IOCE),*G8 Proposed Principles For The Procedures Relating To Digital Evidence*,(online): http://www.ioce.org/core.php?ID=5

[7] Llaneza, P. and Lazaro, F., Evidencias electronicas: de la informacion a la prueba electronica. *Revista Seguridad en Informatica y Comunicaciones (SIC)*,2009, no. 83, pp. 92-97. (In Spanish)

[8] Xu, W., Trappe, W., Zhang, Y. and Wood, T. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,*Proceedings of MobiHoc'05*, ACM, 2005.

[9] Kargl, F. *et al.*, Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications Magazine*,2008, vol. 46, no. 11, pp. 110-118.

[10] Scheuer, F., Posse, K. and Federrath, H., Preventing Profile Generation in Vehicular Networks, *Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing*, 2008, pp.520-525.

[11] Papadimitratos, P. *et al.* Architecture for Secure and Private Vehicular Communications. *Proceedings of the 7th International Conference on ITS*, 2007, pp.1-6.

[12] Buttyán, L. and Hubaux, J.-P, *Security and cooperation in wireless networks*, Cambridge University Press, 2007. ISBN: 9780521873710

[13] Angluin, D., Fischer, M.J., and Jiang, H., Stabilizing Consensus in Mobile Networks. *Lecture Notes in Computer Science.* Springer-Verlag, 2006. núm. 4026, pp. 37-50.

[14] Nai-Wei, L. and Hsiao-Chien, T. Illusion Attack on VANET Applications. A Message Plausibility Problem. *Globecom Workshops*, IEEE Computer Society, 2007, pp. 1-8.

[15] Raya, M. *et al.* On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. *INFOCOM 2008. 27th Conference on Computer Communications*. IEEE Computer Society, 2008, pp.1238-1246.

[16] Wex, P. *et al.* Trust Issues for Vehicular Ad Hoc Networks. *Proc. of IEEE 67th Vehicular Technology Conference (VTC)*, 2008. pp.2800-2804.

[17] Raya, M., Papadimitratos, P. and Hubaux, J.-P., Securing vehicular communications. *IEEE Wireless Communications*, IEEE Computer Society. 2006, vol.13, no. 5, pp.8-15.

[18] Raya, M. and Hubaux, J.-P., Security aspects of inter-vehicle communications. *Proceedings of the 5th. Swiss Transport Research Conference*, 2005.

[19] Rahman, S.U. and Hengartner, U., Secure crash reporting in vehicular Ad hoc networks. *Proc. 3rd Intl. Conf. on Security and Privacy in Communications Networks*. IEEE Computer Society, 2007, pp.443-452.

[20] Young, C-P., Chang, B., Lin, J-J. and Fang, R-Y. Cooperative Collision Warning Based Highway Vehicle Accident Reconstruction. *Proc. 8th International Conference on Intelligent Systems Design and Applications*, 2008.

[21] Lin, X., Sun, X., Ho, P-H., and Shen, X. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications, *IEEE Transactions on vehicular technology*, vol. 56, no. 6, November 2007.

[22] Raya, M., Aziz, A. and Hubaux, J.-P., Efficient secure aggregation in VANETs. *Proc. 3rd international workshop on VANETs*. ACM, 2006. pp.67-75.