POLYTECHNIC UNIVERSITY OF CATALONIA

MASTER THESIS

A reputation-based scheme for announcement messages in vehicular networks

Author:
Jaime SANTOS

Advisor:
Jordi FORNÉ

Department of Telematics Engineering
Barcelona September 7th 2011

Acknowledgments

I am heartily thankful to my supervisor, Jordi Forné, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.
I also offer my regards to all of those who supported me in any respect during the completion of the project.

Contents

List of Figures

List of tables

Summary

Vehicular Ad-Hoc Networks (VANETs) are shaping up as the next step to provide information and safety services to vehicles. These networks are characterized for being variable in terms of connectivity and delay due to continuous changes in the topology. These conditions are acceptable for developing best effort information systems, no bounded in delay or rate. However, when dealing with critical safety applications, as emergency accident reports, some improvements are needed in terms of reliability and security. In this thesis, we present and classify the incoming VANETs services and the techniques to enable nodes to trust their neighbours' announcements in an efficient and secure manner. To overcome the limitations, we propose a reputation-aware system for VANETs based on digital credentials conveying the reputation value assigned to users. Finally we evaluate the costs and accuracy of this new proposal by itself and combined with the existing ones based on revocation lists.

Keywords: VANETs, certificates, credentials, reputation, trust.

1 Introduction

Vehicular Ad-Hoc Networks (VANETs) constitute a promising technology emerged from the application of Mobile Ad-Hoc Networks (MANETs) techniques to the interactions among vehicles equipped with a new generation of communication devices. It is aimed to deliver a vast range of services: from comfort applications, such as traffic information, automatic toll payment or even plain Internet, to safety functiox nalities as driving assistance or crash notifications by means of a dynamic and self organized network where the vehicles themselves form the infrastructure and sense their medium to collect information to be shared. We will go in detail through all of the possible services in the background section.

Proven the growing pace of VANETs, regulatory bodies and projects have been established to introduce some standardization and coordination: C2C-CC (Car2Car Communication Consortium)[2]: It is a non-profit organization launched by vehicle manufacturers in Europe in 2004. It proposes realistic deployment strategies and business models to speed up market penetration. Some remarkable projects are: PreVENT, FleetNet/NOW and SeVeCom. In USA, Vehicle Safety Communication Consortium (VSC) and IntelliDriveSM (formerly known as Vehicle Infrastructure Integration) are major initiatives for establishing the use of common frequency band to get "communications to deliver timely information to save lives, reduce congestion and improve the quality of life" [3]. Advanced Safety Vehicle (ASV) and Advanced Highway Systems (AHS) constitute the Japanese approach, where public sector builds the basic services for information and safety and supports the deployment of a vast fixed and on-board Ad-Hoc network infrastructure. The technology used is the 5.9 GHz Dedicated Short Wave Communications (DSRC) and, at least, the ASV project, is aimed to be compatible with C2CC.

The aforementioned radio technologies are mainly based on an amendment to the IEEE 802.11 standard: the 802.11p. It contains some enhancements to support Intelligent Transportation Systems (ITS), data exchange between high-speed vehicles and between them and the roadside infrastructure in the licensed ITS band of 5.9 GHz

Despite its particularities, VANETs, as any other networks, need appropriate routing protocols to deliver the information. Due to the common roots they have in wireless sensor networks with MANETs [4], they inherit some of the flavours of the routing techniques with some modifications. Ad-hoc networks routing normally disseminates information. Whereas, considering that VANETs are aimed to have

infrastructure support, some hierarchy and addressing is present. This is not the object of this work, but enough to be said that cars are particularly suitable for Location Based Services (LBS), so routing protocols can leverage the availability of GPS positioning systems, which in terms of routing facilitates directing information to the physical areas where the destination is more likely to be.

We need consider the drawbacks and the advantages of vehicular networks: in one hand, despite its movement is constrained by roads and others physical elements,it still depends on the social behaviour (sometimes difficult to be modeled). Besides, there are negative radio propagation effects due to buildings and other obstacles, so network stability is an important issue. Whereas, on the other hand, we have to remind that, if successfully deployed, VANETs can provide a potential number of millions of long battery distributed nodes almost anywhere near persons. This conditions lead us to consider an added value on this technology, which will not only provide driving safety, but also will increase the number of access points to Internet, with all the services associated. This way, in a near future, VANETs, mesh networks, WiFi hotspots, WiMax and cellular networks would work together to provide continuous and seamless connectivity. It is an exciting future than worth to be researched.

In such a distributed network as VANETs propose, nodes need to be collaborative, but then security becomes critical. A user will only choose to share their resources (connectivity, information, computation power) if encouraged with a decent level of security, that is: if there is 'trust'. Nobody will take the risk of collaborating without some guarantees. This security can be achieved by efficient authentication methods and elaborated trust reputation systems. In this work we will focus on the state of reputation techniques in the area of VANETs and will propose some improvements.

The remainder of the paper is organized as follows. The Background section gets some insight in the state of the art of VANETs services and the application of reputation to improve their performance, then continues the Contribution section with a proposal for improving the accuracy of the reputation, based on the use of new certified entities: the Reputation Certificates. The Evaluation section compares the existing techniques with our proposal and its followed by a Conclusion section presenting some assessments and open issues.

2 Background

In this section, we first will gain some insight into the different services to be deployed by VANETs, once this technology is fully implemented. We will review the physical requirements needed. One of the most important aspects is security, which can be accomplished by using reputation systems. We will show that, as the interactions among users in VANETs are sporadic an irregular, a careful design is mandatory. Distributed reputation approaches are difficult to implement and some kind of centralization should exists.

2.1 VANETs services

Inter-vehicle communication can provide a vast range of services that will cover all applications already provided by devices such smart phones or laptops plus all those related with driving safety. Depending on the authors, there are different classifications. A common one is based on their criticality, beside its character periodic or event-triggered Table 1.

Table 1. Examples of VANETs services

Comfort applications	Safety applications	
	Event driven	Periodic
Traffic info. systems	Obstacle detection	Time-stamp messages
Weather information	Hazardous road conditions	Vehicle parameters beacons
LBS	Post crash emergency call	Road signal information
Internet access	Emergency Brake Warning – EBW [5]	Parking information [6]
Toll payments	Intersection Collision Warn. - ICW[5]	Opportunistic routing

• Comfort applications: Intended to provide information about weather conditions, traffic congestion, parking alerts and so on. We can find an inter-vehicle, group communication or a communication to a central database, where distant and/or disjoint information can become meaningful. Characterized for having a very wide broadcast area and loose authentication constraints, which could be provided at the application layer (e.g.: SSL connections for Internet access).

• Safety applications: They have priority over comfort applications. Related to the detection of hazards on the roads and sending advises locally to other drivers. Include

sudden braking of cars ahead, slippery pavement, reduced visibility or obstacles on the road . We take for granted that vehicles can detect those dangers and/or measure the related variables by themselves in the very near area. Nonetheless, receiving security advertisements from neighbours increases safety dramatically.

Safety services are much more demanding in terms of security (authentication, trust) and time delay. They are triggered by events and certain actions must be taken on response to avoid a risk to be materialized under very strict delay conditions.

Security announcements commonly warn about local hazards, so the transmission area is close to the point where the event happens and broadcast transmission is normally used. A clear example is the security announcement service.Table 2 shows a summary of the physical and security network requirements according to the state of art solutions for three typical safety-related services.

Table 2. Typical parameters for VANETs services

	Broadcast area	Packet size	Nodes	Delay	Retransmission	Authentication
EBW	300m[1]	500B	10	<500ms[2]	No	Important
ICW[3]	< 100m	500B	10	<360ms[4]	Yes	Important
Time-stamp	< 100m	500B	< 4	<300ms[5]	Yes	Recommended

In the present thesis, we focus on the Emergency Brake Warning (EBW) service as we believe it is representative of critical security announcements and requires the use of reputation and decision techniques. Besides, due to the characteristics, it allows longer users interaction that for instance 'obstacle detection'. This is important when reusing some credentials to make the subsequent interactions faster.

Our aim is to evaluate the current techniques which try to assure that these services are delivered securely. There are various proposals, but is quite commonly accepted that there should be a centralized Trusted Authority (TA) that gathers data from the cars population to create the individuals reputations and also enables a distributed deliver that reputation. This is based on credentials and certificates that can be interchanged among the actors without a continuous intervention of the TA.

1 300m according to [15]

2 GPS position time generated in 200 ms. Average human reaction 700 ms

3 Services defined in [5]. According to it the urban scenario is the worst in terms of demanding faster response and more congested communication medium

4 The maximum delay is calculated from a typical urban crossroad, one user approaching at the maximum allowed speed (50km/h). This is derived from the maximum broadcast area which is determined by modulation and for a sure delivery of the packet.

5 According to DSRC

2.2 Reputation Systems

Building trust relations is a key part of today's distributed systems. They increase the efficiency without having to improve the detection or actuator parts whereas they are critical to avoid bad behaved users to stay in the system with impunity.

There is an extensive literature on those systems but for our scope we will focus on the hybrid-decentralized reputation ones. This is due to the fact that VANETs systems need reputation regarding inter-vehicles relationships (which can be reported to a coordinator) and also because wireless systems make impossible to request others' reputation for all and each announcement.

Some proposals as VARS [7] recommend to use a system not dependent on a a Trusted Third Party (TTP) to manage the reputation, as most of the VANETs networks are highly heterogeneous and experience connection variability. In this suites, an opinion based on the experience is appended to the message as it is locally forwarding by the vehicles. We believe that, despite some promising results, it adds excessive complexity to the system and assumes poor connectivity which in the near future will be overcome.

Regarding the hybrid reputation management systems, here we cover the role of the TTP as a Certification Authority (CA) that delivers not just Digital Certificates but also, as a novelty, another kind of certificates containing information about reputation. We envision a trust scheme in which nodes inform about others behaviour to a TA which builds up a scoring database with the nodes' ranks. With these data, two kinds of certificates are made: the classical Identity Certificates(IC) and a reputation certificate based on credentials. This latter is based on the existing Attribute Certificates, containing in their extension field a value that represents the reputation of the emitter node. This way, the node can show a certificate to validate himself for being trusted in front of others and regarding a certain service.

Both kind of certificates will be updated when necessary or revoked (explicitly or not renewed) when the user reaches some degree of bad behaviour. Also a node can be expelled from the network or banned from some services due to various reasons: Inefficient or harmful use of network resource; exceeding of bandwidth usage; not relaying other nodes information; false announcements or no proper collaboration in routing tasks. We will detail this approach later on.

2.3 Certificate verification

As is stated in the survey [3], the announcements from a group of vehicles and more generally any VANETs security service needs some kind of authentication to avoid that malicious nodes to impersonate members of the group and send fake or incomplete information (road sliding status, presence of an accident and so on).

This authentication can be achieved by means of Digital Certificates. For wired communications, these certificates are normally interchanged at the beginning of a secure communication as a prove of authenticity, enabling to interchange securely information by Public Cryptography techniques and setting further session keys.

However in VANETs the scenario is a little different. We do not pursue long secure communications but short authenticated announcements. Cars are moving constantly and their interactions will be quick, in terms of seconds or minutes at most.

So a first approach is to append a certificate to every single message, which in turn is signed with the correspondent private key (pair of the public one contained in the certificated). Providing the CA's public key is publicly recognized, the receiver can verify the authenticity of the certificate and. as a consequence, the authenticity and integrity of the message.

Despite recognizing the authenticity of the CA's public key we need to know if, since the certificate was issued, the CA is still recognizing it as valid. This will lead to a constant verification of certificates/signatures, one for each message broadcasted. Considering that services as the time-stamp need a periodicity of 300ms [8] and the usual vehicles densities in big cities, we see that the typical certificate verification techniques will require some modifications to cope with this huge amount of verifications.

A feasible solution is the collaboration of near elements: Road Side Units (RSU) or even some designated cars. Therefore we need efficient protocols capable also to work with non reliable elements, as they are more numerous,cheaper and closer to a random user.

To accomplish the verification we have two approaches: We can use advanced certificate status validation techniques as the one presented in [9] to compare the certificate to a trusted list of annulled certificates. Users receive the announcement with the Certificate attached and before processing it, they query about its state by asking to a close node (which has a fresh list of the revoked certificates). Instead of downloading the whole list, just certain parts of a previously built hash tree are transferred to verify the certificate's status regarding the reputation, which speeds up the process. If the certificate is valid, then the node that receives the announcement can proceed to check the message's integrity and authenticity. For this approach to be efficient, we need some nodes in the vicinity that could acting as repositories, an

appropriate Service Discovery Protocol (SDP) to be aware of them and some grade of connectivity to make possible to download the lists to certain nodes

Other methods of authentication change the paradigm and use the batch verification of signatures. As in VANETs announcements there is a broadcast common space under an RSU coverage area where all the vehicles are transmit messages, it makes sense that sets of signatures can be verified altogether. One interesting approach that offers this service is SPECS [10], which is a very complete suite providing signature verification by interchanging secrets between OBUs, RSUs and TA and making use Bilinear Pairings for the cryptographic operations. The advantage is its robustness and a quite bounded delay, whereas its main drawback is its complexity and the continuous interchange of information among the three aforementioned elements.

3 Our contribution: Service reputation by digital credentials

So far, we have a view of the existing techniques for adding security to the announcements in VANETs and we know that is worth to have an hybrid system where the TA holds and delivers the reputation. Now our aim is to extend the concept of reputation. Not just having a 'accepted or not' decision, but a gradual reputation, with different levels, able to trigger diverse reactions in the objective node. We believe that a partly centralized system provides several advantages:

- Better approximation of users behaviour. As it receives feeds from different users interacting to the target in different locations and circumstances, it will be able to weight them accordingly. E.g.: A system can decide to rely more in the reports of vehicles with newer sensors and less in other whose sensor reports malfunctioning.
- Flexibility. The deliverance of certificates containing reputation can be achieved through the same infrastructure used for the identity certificates. Only the reports about other users behaviour will need to be planned, but, as it is not timely constrained, it is not an issue. In addition, any improvement in the reputation calculation algorithm can be done seamlessly as it all resides in the TA, not in the nodes themselves.
- Reliability. So far, completely distributed system have been proved to be excessively prone to be attacked. A group of malicious nodes could manage to create false reputations leading to critically dangerous situations in safety driving applications.
- It results more accurate and also easier to control. Bearing in mind that sometimes in the driving environment, a low reputation may imply legal implications as well. So, in case of serious offences, the legal authority could ask the TA to disclose the reputation and location history of certain drivers.

We will see some of the expected characteristics of the system we propose from its general architecture, the gradual responses that the users can show to different levels of services reputation and finally to the security entity that can help in delivering the reputation in an efficient manner.

3.1 System's overview

As we mentioned in the introduction, our system will be based on an enhancement of the Wi-Fi protocol for vehicles inter communication: the 802.11p. When dealing with security announcements, the nodes (vehicles) interchange short messages regarding different events in their vicinity and also communicate to central management elements to verify the authenticity of others information or to request certificates to enable them to send secure messages.

As all the aforementioned certificates must be issued by a TA which also has to receive the reports from the vehicles, a clustering architecture is a good option. There will be not just a TA but a central one and several local TAs all linked by secure and high speed connections forming a clustered configuration Figure 1.

A set of cells, controlled by a Wi-Fi Access Point, also known as Road Side Unit (RSU), will be deployed depending on the vehicles population, most of the times reusing existing cellular base stations of municipality hotspots. All the security sensitive processes will take place either on the nodes or in the trusted elements (TA), therefore the RSUs can be built over no so-reliable elements, making a fast deployment easier. The RSU can connect to the TA by a point to point connection over a plain HDSL line which nowadays can provide quite realistic symmetric rates of 1Mbps at a low cost.

All of the TAs are entrusted to sign the certificates and will receive encrypted lists about the local vehicles which certificates have to be issued. They will also receive reports from the vehicles under their domain and will aggregate that values to save bandwidth on the path to the root TA.

In Figure 2 we can see a summary of the overall system structure with some elements as the reputation certificates that will be explained in the immediate sections.

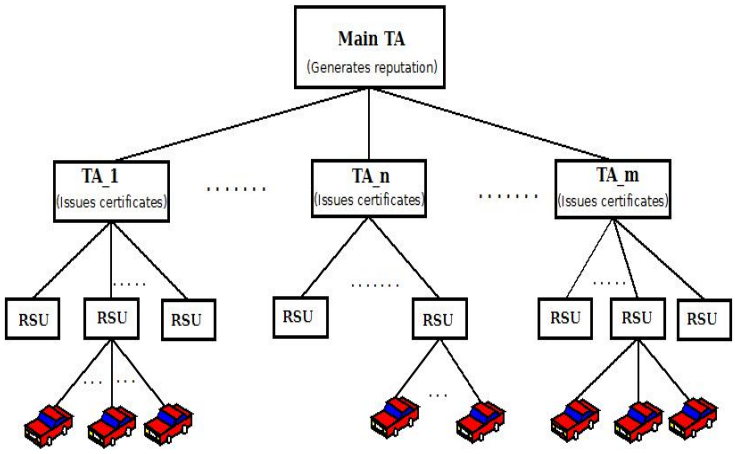

Figure 1. Clustered TAs configuration

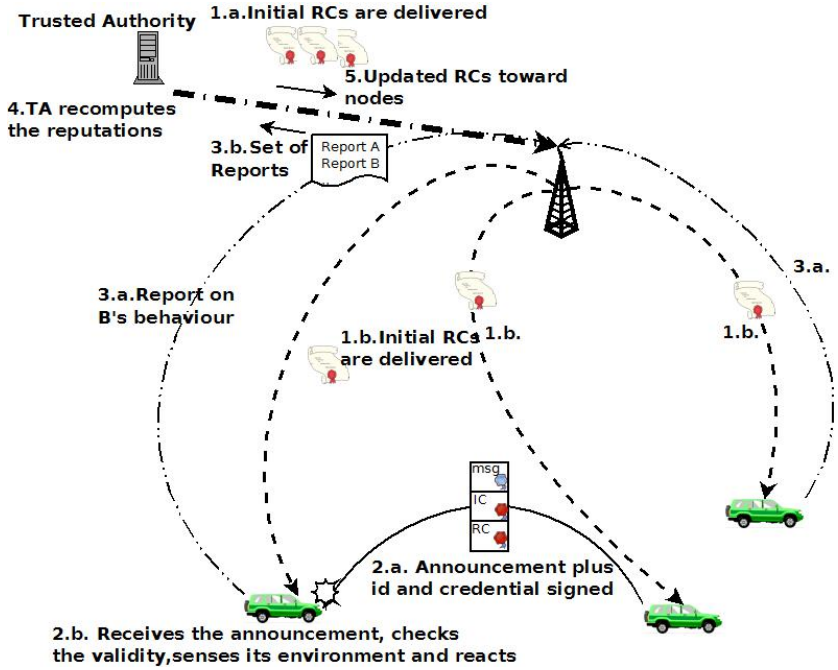

Figure 2. System architecture

3.2 Service's granularity

To complement the global reputation and leverage the vehicle's sensing capabilities we define an architecture that decides on the basis on a combination of both local and global reputations.

Services can be announced with different grades of certainty, proportional to the user reputation, so the response to them can be modulated, taking more or less expeditious actions. This way, the decision module has more flexibility and even the less trustful data, can be use for even small adjust, so the efficiency increases. As we see in the Figure 4, upon the reception of an announcement, the a local trust is combined with the global reputation and is processed by a decision module which produces an appropriated response to the announcement. These three elements are in a trust framework or context, which means that, depending on the node conditions, local or global trust could be modulated.

As an example, the local information comprised by the data collected by sensors as proximity radars, could be explicitly modified by the context in the form of a driver input. A proximity warning system will combine information from the reputation, contained in the own announcement, and also from the car's proximity radar (local information).

Table 3. Actions delivered according to announcement trust

	Trust range: 0 – 0.3	Trust range: 0.3 – 0.6	Trust range: 0.6 - 1
Obstacle proximity (EBW,ICW)	Dashboard 'caution' light	Indicator light and sound plus data (approach direction, speed) Brakes and air-bag and other securities ready to be activated	All indications plus automatic assisted brake activation
Hazardous weather	General hazard indication to the user.	Warning detailed information is shown to the user with suggestions about the actions to take.	Warning plus automatic actions (brake activation..)
Post Crash call	Receiver verifies in emergency center	User is notified about the emergency and related data	User notified plus related data
Time-stamp	Plain gps position	Position, speed	Position, speed and added services

3.3 Reputation information delivery

As we have seen, the bandwidth associated with the data interchanged to verify the certificates can be bounded, providing we have enough RSUs scattered throughout the roads. However, we have to distribute the information regarding the users reputation in a manner that the individuals information stays updated but the whole system is not excessively overloaded. This part of the architecture has to be designed carefully as, the inter-vehicle radio interface is hard to model and suffers from unexpected phenomena, being difficult to guarantee a minimum data rate.

We have two information units that need to be transferred to articulate the reputation's deliverance:

• Certificates' Revocation Lists (CRL): They are big files containing information from nodes expelled from the system either because they are not enabled to stay inside (identity revoked) or because their behaviour has led them to an forbidden situation (reputation revoked). These lists of nodes are periodically transferred to repository nodes, used to quickly check the status of the certificates. They maintain a 'yes or no' information, so their reputation information is limited but their distribution is easy. Different techniques allow to check those lists remotely and in a secure manner, with no need to download all their elements [9].

• Credentials: They bear more accurate reputation information (e.g.: real number from 0 to 1). However, as there is one for each OBU, an uncontrolled massive distribution could easily make the system collapse. It provides detailed information but needs a planned distribution. At the end of this section we will depict how this credentials can be implemented with a entity based on the Attribute Certificates.

An additional property of the certificates can be exploited: the validity period so we can set two strategies: Certificates with a fixed and long validity period and Certificates with short and variable validity periods.In the first approach, the certificates are delivered in periods of time when the network's activity is low, let's say during early mornings (from 0h to 6h).

The second approach tries to adapt the certificates life time to the forthcoming user's behaviour. That is, if a user is stable in its actions, normally a certificate will be longer as is more likely that reflects its actual situation, without needing to be renewed. However, if a users changes its behaviour, more frequent, shorter life certificates will better reflect its state. The announcement producer knows that no service is valid with outdated certificates, so it will wait for the newly used one to broadcast its services. Therefore, the TA will change the validity period according to reputation changing pace.

$$Validity\ period\left(t+\ \Delta\right)=\left(\ \alpha\cdot\frac{d\left(Reputation\right)}{dt}\right)^{-1}$$

This approximation follows a plausible supposition that most of the users reputation will follow a smooth changes. So most of the users will have their certificates reissued and delivered in widely spaced periods, not overloading the system. Only those whose reputation rises or falls sharply will have more frequent deliveries. Additionally, if the system detects that the number of certificates delivered is very high, it start discarding the renewal of those falling fast, so the cars that are behaving continuously bad, can experience periods of no service, while there is room in the system to receive their certificate, this is known as false positive, a 'lesser evil'.

3.4 Decision module

When a car receives a security announcement from a nearby vehicle, before making a decision any action, it checks both certificates: the certificate related to identity, to be sure she is a legitimate user, and then the reputation one to check if we can trust her service. These certificates can be verified against the TTP by communicating to it and checking their status or also they can be trusted straight away through short life certificates that need to be renewed frequently. We will study both approaches for different services and environments

To introduce more flexibility to the system's decision module, we consider not only the different levels of reputation that can be provided by the information in a certificate, but also we see different levels of response to the announcement by the receiver node, that is a service granularity Figure 3.

In this way, the receiver can match an announcement with rank, combined to local observations and a context with the proper level of service. E.g.: When receiving an announcement about 'very slippery road 1 mile ahead', the system reads a reputation rank of 0.65 out of 1. According to Table 2 we are in the trust level 3. However let's assume that we have on-board sensors that work correctly and produce a result of 'slightly wet road'. With this and other data, the decision module would consider the announcement in the trust band 2 and apply the action according to this less trustworthy state: “Warning detailed information is shown to the user with suggestions about the actions to take”

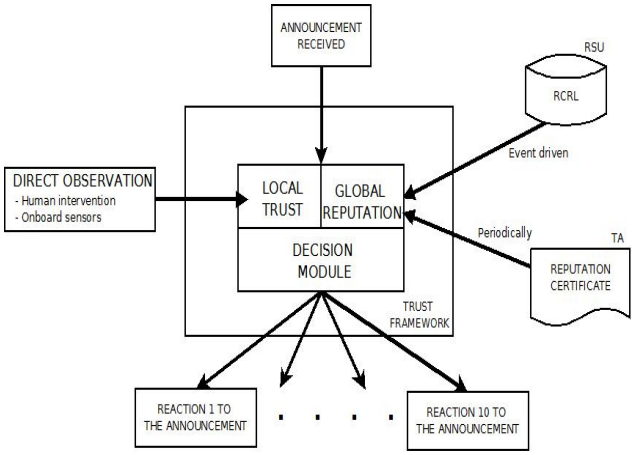

Figure 3. Decision module in the OBU

3.5 The Reputation Certificate

As we have reviewed, in the state of the art, nodes can check others announcement and verify their validity. This way, the TA qualifies the nodes as revoked or non-revoked after gathering the opinions and building a binary state from a certain reputation model. However, this binary status strategy is not flexible and makes hard to accommodate a big range of services to the security paradigm There are complementary sources to build more accurate reputation as chain of trust among local nodes or polling systems that collect opinion in the surroundings [11]. Nevertheless, VANETs are characterized by sporadic and short interactions among users, sometimes too few to build autonomous reputation ranks with enough reliability.

We envision a hybrid system that listens the reports, builds individual user's reputation and delivers it in the form of certificates. These certificates will afterward be delivered among users, being this the 'distributed' part of the approach. A common system for all the vehicles, if properly designed in terms of security services and having an adequate network dimensioning, would have a much better resilience.

Following the aforementioned requirements, we introduce a scheme for providing each user with a reputation mark that qualifies the services it offers. To avoid malicious users to forge about this mark, it has to be bound to their identity and to the own message. As a consequence an announcement will not be valid without it.

So the entity that fulfills the enumerated requirements is the commonly known digital certificate, now adapted to be used with reputation. Each messages will be identity certified by the known IC and also reputation will be certified by a Reputation Certificate (RC) linked to the IC. This new element is issued and signed by the TA. Whereas IC binds a user identity to its it public key and backs this information with the CA signature, the RC is an attribute certificate type that binds the user current rank with the user identifier provided in the IC.

Based on the standard structure of an attribute defined in [13], RC will look as seen in Figure 4. It follows the scheme of an Attribute certificate but adding a new kind of extension with one byte, expressing a reputation mark going from 0 to 1.

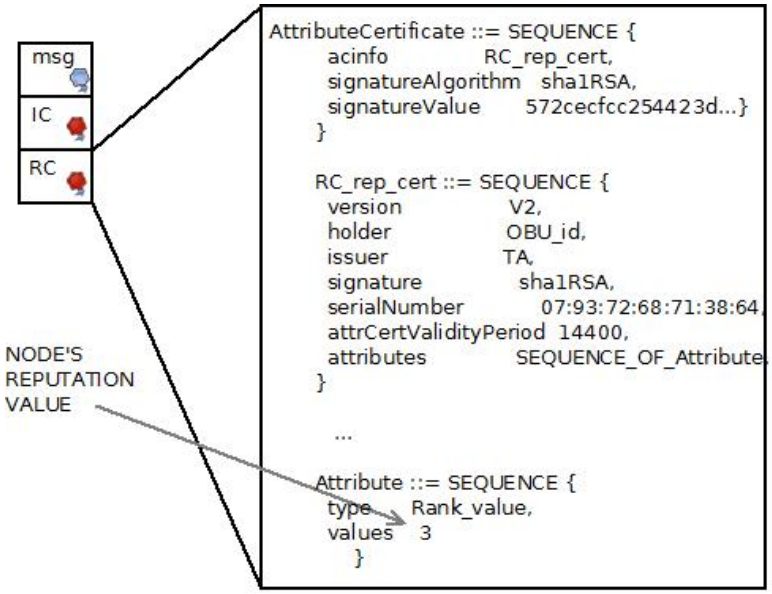

Figure 4. Reputation Certificate ASN.1 notation

4 Evaluation

Now we will compare the different scenarios for delivering trustworthy reputation to VANETs, based on the newly introduced RC combined with the existing certificate status validation techniques.

We will evaluate the differences in computational cost due to the cryptographic operations in the OBUs, the cost of bandwidth either in sort distance communications vehicles-RSU and in the fixed links from TA to the OBUs and finally some comments on how accurate each of the systems are.

For establishing a framework of study, we assume a system already using IC, with a trusted CA/TA whose IC is known and accepted by all the users. Users keep an IC with a long validity period, let's say years, which only has to be reissued when it expires or in case of a serious offence.

Nonetheless, when the cost of issuing and distributing the ICs is considered negligible (as the probability that lots of drivers have their identity revoked simultaneously is low and even in that rare event) its distribution could be properly scheduled for not to overload the system.

We also consider that the IC revocation status validation is accomplished by a batch-type signature verification following the SPECS suite [10]. Therefore its cost in terms of delay, operations and bandwidth is known and bounded as we will refer when required.

For our study we consider a cars population of 900,000 cars, 10 % of the cars having their RC revoked and 50 % per cent of cars in movement in a rush hour. The RC size can be roughly approached by 1kB. We also consider that the TA can compute overall parameters as the average reputation value Rep_{AVG} and the overall reputation loss rate $Loss_{AVG}$. The values will be used in these and the other two schemes to have a value of the system total accuracy.

As the cars interact, they offer and receive services (announcements) among them. At the completion of each announcement, the receiver can compare the parameters the emitter set in the announcement with those variables sensed by its own sensor in it vicinity. According to it, the service can be 'ranked' and its result be reported towards the TA.

The reporting messages are not covered in these work but is worth to mention that they have to be signed to verify their authenticity and avoid attacks by faking reports and also that they should be spaced in time for not to saturate the system. A good option would be to store locally and report groups of them with the initial authentication messages that are interchanged upon the arrival of a new OBU to an RSU coverage area.

4.1 Long life RCs and certificate status validation

In this scenario, in one hand we have the verification mechanism which gives the user a 'revoked/no-revoked' information after consultation. This is just an approximation to the reputation value so the receiver OBU just knows whether the certificate is valid or not. The advantage of this approximation is its speed and effectiveness, as it is implemented by batch signatures verification or checking revocation lists. The system, whose revocation lists are stored in the RSU, can be renewed more frequently than delivering individual certificates.

Besides the coarse certificate status validation, we have the fine approximation to the reputation value: the RCs, which are delivered individually to each user who, later on, will attach to its announcement .

Regarding the BW used in the fixed links from the TA to the RSUs, we can observe from Figure 5 the contribution from the deliverance of both revocation list (RCRL) and the Reputation Certificates (RC). For comparison to the the other schemes, we can say that the $BW_{TA \rightarrow RSU}$ is in the range from 400Kbps to 900Kbps.

To calculate the bandwidth inside the cell, we have three elements: the BW for delivering the RC and reporting other user's behaviours, the BW for downloading the revocation lists and BW for interchanging message plus certificates in the own announcements.

The RCs can be delivered once a day, during the hours or low activity (let's say from 0h to 6h) and, if properly scheduled, it will have little impact on the local BW. Also the reports can be scheduled, they do not need to be continuous and can be grouped, reporting lots of informs in just one transactions, so we do not consider them noticeable.

For the rest of the elements, we consider an RSU cell of 300 m containing 300 cars. On average, we consider that one car produces 4 announcement per second, being each announcement approximately 2kB message's body plus IC and RC). In an urban or semi-urban area the announcements are referred to events happening in user's vicinity and also aimed to users nearby. We can use this fact to avoid an storm of announcements that would be unbearable for the DSRC standard **[15]** by sub-dividing the cell in emission parts. This can be easily achievable by limiting the emission power when sending local announcements but using higher power when transmitting towards the RSU. So if we divide a 300 m diameter cell in 8 parts , as we we get a BW of 2,2 Mbps.

For computing the BW for the reputation certificate status validation checking we use the method stated in [9] which allow us to use repositories to deliver the revocation status even more locally (just in a femtocell of 70 meters around the repository cars). The cost of this local information if we consider 35 cars in 70

diameter femtocell, 4 requests per second and the length of the verification information for [9], we get a BW of 1,4Mbps. Therefore the total bandwidth is $Bw_{cell_RC} \simeq 4$Mbps. Regarding the Time/cpu cost due to cryptographic operations, to get some insight into the cost that the security mechanisms add to the system, we inspect the different steps from the arrival of the signed announcement until it arrives to the decision module (or is discarded) Figure 7. In the Table 4 we can see an approximation to the processing times in a state of the art equipment based on the study of [14]. We consider the cars' equipment is more powerful that the one in MANETs/WSN, approximately like a desktop PC.

Regarding the system's fidelity to reputation, if $Loss_{AVG} \cdot Tr > Rep_{AVG}$ there is 'impunity period' for some nodes (but Tr is considered fixed in this scenario) Figure 6

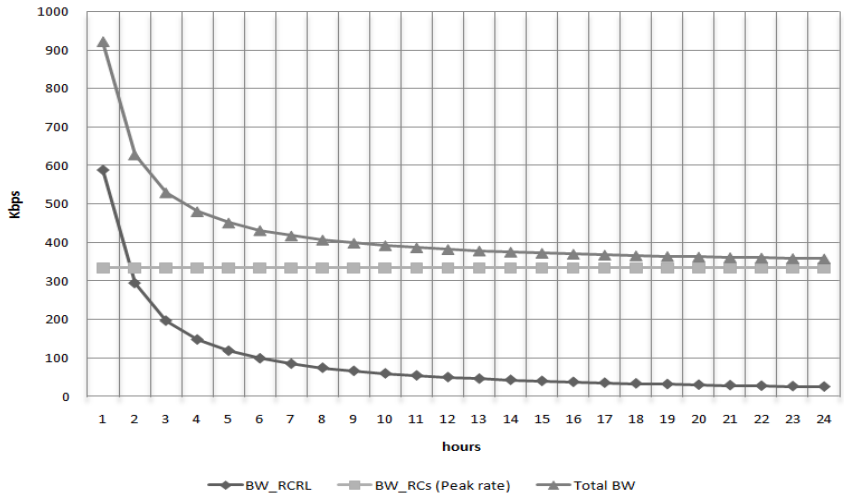

Figure 5. BW from TA to RSU

Table 4. Time cost for cryptographic operation. RC and certificate status validation

Security operation	Description	Time(ms)
IC revocation status checking and signature verification	SPECS suite [10]. Batch verification, Bloom filter, Bilinear Pairnings	15ms
Message signature verification	ECDSA_2048	3ms
Certificate status validation based on [9][15]	2 x Tx time RSU↔OBU plus SHA1 and ECDSA_2048	1+1+3+0.1 = 4.01ms
RC signature verification	ECDSA_2048	3ms
Total		26,01ms

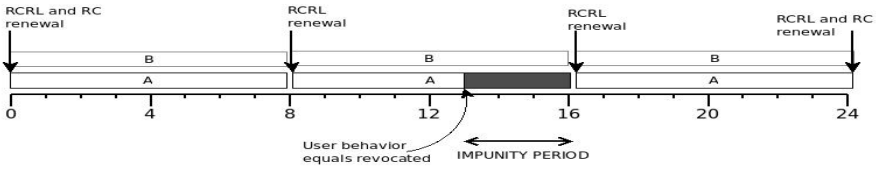

Figure 6. Effect in time of a short CRL renewal period

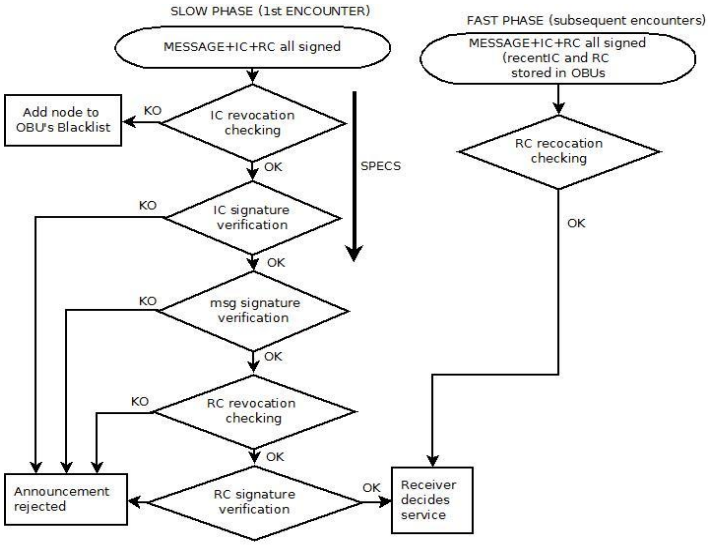

Figure 7: Steps security announcement for RC plus status verification

4.2 Fixed validity period RCs

Here we consider a system relying just in the RCs, which are delivered individually to each user. The validity period for the RCs is fixed but their delivery to all the population is distributed over the period to minimize peaks in the rate.
This system is less difficult to implement, as most of the elements to produce, delivery and handle the identity certificates are already deployed and can be reused for the RCs.

Bandwidth cost from TA to the RSUs through the fixed Internet links varies with the RC renewal time Figure 8.

To approximate the BW inside the RSU cell, we follow the approach of the previous section [15]. With 8 broadcast areas inside each cell and we get a BW 2Mbps. The other exchanges that could affect in the local BW are the vehicles behavior reports (very low as explained in the previous case) and the delivery of RC plus some secure delivery protocol will still be a low rate, let's say 50 kbps per cell. Therefore, we have $Bw_{cell_RC} \simeq 2{,}05$Mbps.

Regarding the cost of the security operations we can observe it decreased as now it is not necessary to check the validity of the users on this reputation. We can say that now this is implicit in the existence or not of the RC.

Systems fidelity: Alike the previous case, if $Loss_{AVG} \cdot T\_update > Rep_{AVG}$ there is an "impunity period' for some nodes (but Tr is considered fixed in this scenario). Nonetheless, when referring to long renewal periods, the values $Loss_{AVG}$ and Rep_{AVG} do not reflect reality. If we use a day renewal, it is more likely that a part of the users will be able to operate in a revoked situation.

There is also a less critical inaccuracy due users offering services out of their real reputation band. As a result, the system's accuracy is improved from a fixed validity period scheme or even from a homogeneous variable validity period.

Table 5. Time cost of the cryptographic operation with sole RC based systems

Security operation	Description	Time(ms)
IC revocation status checking and signature verification	SPECS suite [10]. Batch verification, Bloom filter, Bilinear Pairnings	15ms
Message signature verification	ECDSA_2048	3ms
RC signature verification	ECDSA_2048	3ms
Total		21ms

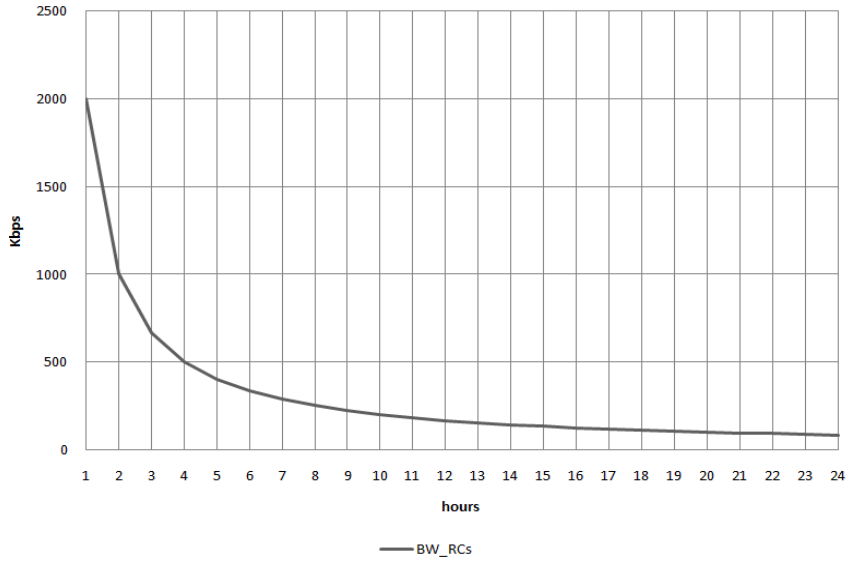

Figure 8. BW from TA to RSU

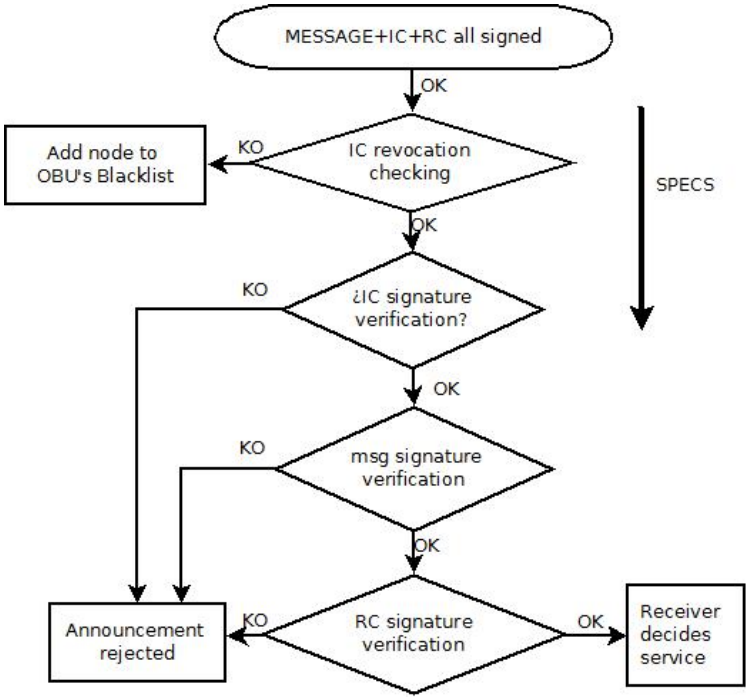

Figure 9. Steps security announcement for RC scheme

4.3 Variable validity period RCs

As we commented in the contribution section, adapting the validity period to the previous behaviour can improve the system's quality and decrease the bandwidth, providing users' reputation evolves smoothly. This last supposition may not always be true. Therefore under high load conditions, the system can decide to issue less frequent RCs. The less harmful criterion would be to issue longer validity periods certificates to fast changing users in the upper reputation range while discarding certificates in the lower range by not issuing them frequently nor extending their validity period.

To get the bandwidth cost in the fixed links from TA to RSUs, we model a typical behaviour of the population,establishing that the certificates validity period varies in the range 30 minutes to 4 hours. We suppose that 20% of the moving cars have a fast reputation variation, 20% a medium one and 60% are stable one. Giving them 30 minutes, 2 hours and 4 hours respectability and using Figure 8 we get a $BW_{TA \rightarrow RSU}$ = 650Kbps.

The bandwidth cost inside the cell is composed of two elements. First we calculate the cost in the own announcements interchanged among vehicles. We follow the same principle as in the case of fixed validity period RCs and subdivide the cell in 8 announcement emission areas where cars broadcast their messages and certificates. That gives us a bandwidth of 2Mbps.

The second element is the cost of delivering certificates from RSU to each of the OBUs. RCs delivery has little impact in the BW between RSU and the OBUs. As seen, the validity period changes and consequently, the renewal time. But even in the worst case that all the population approximates to the revocation threshold (and have the shortest validity period of 30 minutes), it will result in a rate about 1Kbps per cell. Therefore the total bandwidth is $BW_{cell\_RC} \simeq$ 2Mbps.

The time cost due to cryptographic operations in this scenario is the same as in fixed RCs.

For the evaluation of the system's fidelity to reputation, as we commented in the architecture introduction, the TA improves the system's accuracy by modulating the validity period of the newly issued RC as a function of the recent behaviour of the owner.

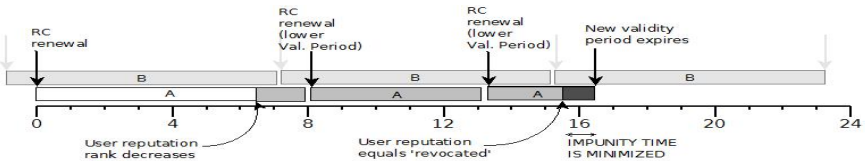

Figure 10. Effect in time of variable validity period RC

4.4 Comparison

For comparison aims, we take $BW_{TA \rightarrow RSU}$ in the range of [0,5 to 1] Mbps as achievable. This rate shouldn't be an issue over a quality HDSL line. For the cryptographic time cost , a figure around the 50ms can cope with the fastest response services, which use to be the brake announcements.

From Table 6 we can see that the differences are in the local bandwidth used by the different approaches and also in the ability to follow the users' real reputation as well as the changes needed to deploy the mechanism

Currently, the DSCR standard allow values up to 4,2Mbps but highly influenced by the traffic load and streets configuration. It is expected that in a near future, better design and protocols will enable the DSCR to deliver these rates and over [16]

Fixed RC has similar cost than RC plus revocation-status-validation but the former is much simpler to deploy as the certificates issuing and processing elements are already present for the IC. However we can see that its quality following the real reputation is not optimal.

'Variable RC' improves 'Fixed RC' in following real reputation values but has a higher cost in BW (4,4 Mbps), nearly in the limit of DSRC. Possible solutions could be: Smaller announcement broadcasting areas (difficult to implement discovery protocols, interferences), Shorter certificates (currently the Elliptic Curves provides the smallest possible), smoother user's behavior (will need real analysis), less announcement rate (some of the services as brake announcement wouldn't be covered).

Table 6. Table for comparison of the different reputation delivery approaches

	$BW_{TA \leftrightarrow RSU}$	BW cell	System's fidelity	Deployment
Long life RC + RC status validation	627 Kbps	3,64 Mbps	High	Difficult
Sort life RC	1 Mbps	2,2 Mbps	Poor	Easy
Variable life RC	650 Kbps	4,6 Mbps	Medium	Easy

5 Conclusion

In this thesis we have reviewed the current mechanisms to efficiently introduce the concept of reputation in VANETs. We have seen that this concept turns specially relevant as these are vehicular networks where safety is critical but also, because of the sporadic users interactions and other factors is difficult to implement a robust and distributed reputation model.

The current proposals, based on certificate status validation lists, offers a limited scope for reputation management as we only know whether the other end is entrusted or not to play a role in the network. We introduced a system based in the principle of identity certificates but applied for the scatter distribution of a centrally generated reputation, so that the certificates are delivered to their owners and they redistribute them with their service offers. In parallel with this smooth reputation, we proposed a gradual response based on the different levels of trust in the services. This is ruled by a decision module which dwells in the cars and also gathers local information from sensors.

Our analysis proved that the reputation certificates are simpler a easier to deploy than other approaches as the distributed reputation or the revocations lists. Besides, compared to the latter it equals or even improves its fidelity tracking the actual user's reputation value.

For further works some simulations should be done for fine tuning the system's parameters and also a study on the techniques based on decision theory and their application for fast response in the car's decision module.

Glossary

AP	Access Point
CA	Certification Authority
DSRC	Dedicated Short Range Communications
HDSL	High bit rate Digital Subscriber Line
IC	Identity Certificate
ITS	Intelligent Transportation Systems
MANETS	Mobile Ad-Hoc Networks
OBU	On-Board Unit
PPP	Pont to Point Protocol
RC	Reputation Certificate
RSU	Road Side Unit
TA	Trusted Authority
TTP	Trusted Third Party
VANETS	Vehicular Ad-Hoc Networks
Wi-Fi	Wireless Fidelity
Wi-MAx	Worldwide Interoperability for Microwave Access

References

1. Gershenfeld, N., Krikorian, R., Cohen, D.: The Internet of Things. Scientific American, vol. 291, no. 4, pp. 76-81, (2004)

2. Car to Car Communication Consortium, http://www.car-to-car.org

3. Daza, V., Domingo-Ferrer, J., Sebe, F., Viejo, A.: Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, vol. 58, Issue: 4, pp. 1876-1886 (2009)

4. Taleb, T., Sakhaee, E., Jamalipour, Hashimoto, K., Kato, N.: A Stable Routing Protocol to Support ITS Services in VANET Networks. Vehicular Technology, IEEE Transactions on, 2007, vol. 56, no. 6, pp. 3337-3347.

5. Haas, J.J., Hu, Y.: Communication requirements for crash avoidance. ACM Proceedings of the seventh ACM international workshop on Vehicular Inter-Networking, Chicago, IL: ACM, 2010, pp. 1–10 (2010)

6. Szczurek, P., Xu, B., Wolfson, O., Lin, J., Rishe, N.: Learning the Relevance of Parking Information in VANETs. ACM Proceedings of the seventh ACM International workshop on Vehicular InterNETworking, pp. 81-82 (2010)

7. Dotzer, F., Fischer, L., Magiera, P.: VARS: a vehicle ad-hoc network reputation system. IEEE : World of Wireless Mobile and Multimedia. Sixth International Symposium, pp. 454-456 (2005)

8. Ostermaier, B., Dotzer, F., Strassberger, M.: Enhancing the Security of Local Danger Warnings in Vanets-a Simulative Analysis of Voting Schemes, ARES The Second International Conference on Availability, Reliability and Security pp. 422-431 (2007)

9. Forné, J., Muñoz, L., Esparza, O., Hinarejos, F.: Certificate Status Validation in Mobile Ad Hoc Networks. IEEE Wireless Communications, Feb. 2009, pp. 55-62

10. Chim, T. W., Yiu, S.M., Hui, C.K., Jiang L., Li, V.O.K.: SPECS: Secure and Privacy Enhancing Communications for VANET. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 28, pp. 160-175 (2009)

11. Jinyuan, S., Yuguang, F.: A defense technique against misbehavior in VANETs based on threshold authentication, IEEE Military Communications Conference, MILCOM, pp.1-7, (2008)

12. Boldyreva, A.: Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. Public Key Cryptography—PKC 2003, 2002, pp. 31-46.

13. Housley, R., Farrell, S.: An Internet Attribute Certificate Profile for Authorization, IETF RFC 3281, April 2002

14. Cheneau, T., Boudguiga, A., Laurent, M.: Significantly Improved Performances of the Cryptographically Generated Addresses Thanks to ECC and GPGPU. Computers & Security, vol. 29, no. 4, pp. 419-431, (2010)

15. Bai, F., Krishnan, H.: Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications. IEEE Proceedings of the Intelligent Transportation Systems Conference, pp. 355-362 (2006)

16. Balon, N., Guo, J.: Increasing Broadcast Reliability in Vehicular Ad Hoc Networks. ACM, Proceedings of the 3rd international workshop on Vehicular ad hoc networks, pp. 104-105 (2006)