RAR: Risk Aware Revocation mechanism for Vehicular Networks

Carlos Gañán*, Jose L. Muñoz*, Oscar Esparza*, Jorge Mata-Díaz*, Juanjo Alins*
Carlos Silva-Cardenas† and Gumercindo Bartra-Gardini†
*Universitat Politècnica de Catalunya (UPC)
†Pontificia Universidad Católica del Perú (PUPC)
Email:{carlos.ganan@entel.upc.edu}

***Abstract*—Vehicular Ad Hoc Networks (VANETs) require some mechanism to authenticate messages, identify valid vehicles, and remove misbehaving ones. A Public Key Infrastructure (PKI) can provide this functionality using digital certificates. In PKI, key management and corresponding issuance and revocation of digital certificates is one of the key issues that have to be solved. The IEEE 1609.2 standard states that VANETs will rely on the use of certificate revocation lists (CRLs) to achieve revocation. In this paper, we analyze the problems of using CRLs in these type of networks. Moreover, we describe the Risk Aware Revocation (RAR) mechanism that improves the traditional use of CRLs. RAR takes advantage of the two distinct channel types in VANETs to increase the freshness of the revocation information. Moreover, RAR allows users to gauge the risk of operating in a VANET when using CRLs.**

***Index Terms*—VANET, PKI, Revocation, Risk.**

I. Introduction

In the last decade, wireless communication between vehicles have drawn the attention for their promise to contribute to a safer and more comfortable driving experience in the foreseeable future. This type of communications have stimulated the emergence of Vehicular ad hoc networks (VANETs) which consist of mobile nodes capable of communicating with each other (i.e. Vehicle to Vehicle Communication -V2V communication) and with the static infrastructure (i.e. Vehicle to Infrastructure Communication -V2I communication). To make these communications feasible, vehicles are equipped with onboard units (OBUs) and fixed communication units (road-side units, RSUs) are placed along the road.

However, the open-medium nature of these networks and the high-speed mobility of a large number of vehicles make necessary the integration of primary security requirements such as authentication, message integrity, non-repudiation, and privacy [1]. Without security, all users would be potentially vulnerable to the misbehavior of the services provided by the VANET. Hence, it is necessary to evict compromised, defective, and illegitimate nodes. The basic solution envisioned to achieve these requirements is to use digital certificates linked to a user by a trusted third party. These certificates can then be used to sign information. Most of the existing solutions manage these certificates by means of a central Certification Authority (CA) [2]. According to IEEE 1609.2 standard [3], vehicular networks will rely on the public key infrastructure (PKI). In PKI, a CA issues an authentic digital certificate for each node in the network. Therefore, an efficient certificate management is crucial for the robust and reliable operation of any PKI. A critical part of any certificate-management scheme is the revocation of certificates. In this sense, it is stated that these networks will depend on certificate revocation lists (CRLs) and short-lived certificates to achieve revocation. CRLs can be seen as black lists that enumerate revoked certificates along with the date of revocation and, optionally, the reasons for revocation.

As the network scale of VANETs is expected to be very large and to protect the privacy of users each vehicle has many temporary certificates (or called pseudonyms), the CRLs are expected to be quite large. Hence, the distribution of CRLs is prone to long delays. Moreover, during the early deployment of VANETs, RSUs may not be uniformly distributed in the network. Therefore, the way of distributing CRLs must be enhanced to ensure that revocation is performed in those delay-tolerant environments. There have been proposed several ways to improve with the distribution of CRLs (e.g. [2], [4]). These proposals intend to make more efficient the distribution of the CRLs, e.g. by reducing its size or using V2V communication. However, none of these proposals deals with the problem of the lack of information about certificates that are revoked during the validity interval of a CRL.

In this context, each CRL contains a large number of recent revoked certificates that (significantly) differs from the previous CRL. The number of new revoked certificates will vary depending on the time elapsed since the previous CRL publication. These new revoked certificates are unkown to the user during the validity interval of the current valid CRL. It is during this validity interval when a vehicle could be operating with a revoked certificate without knowing it. Therefore, in these situations any VANET user will be taking certain risk of operating with an unknown revoked certificate.

In this paper, we propose a mechanism to make VANET users aware of this risk. The main idea is to take advantage of the two distinct channel types in VANETs to communicate this risk. Thus, while not increasing the communication overhead and reducing contention for the wireless medium, we convey useful revocation information to the users in the VANET.

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

II. Issues when using CRLs in VANETs

As mentioned before, for a certificate authority (CA) to invalidate a vehicle's certificates, the CA includes the certificate serial number in the CRL. The CA then distributes the CRL so that vehicles can identify and distrust the newly revoked vehicle. The distribution should spread quickly to every vehicle in the system.

However, the distribution itself poses a great challenge due to the size of the CRL. As a CRL is a list containing the serial numbers of all certificates issued by a given certification authority (CA) that have been revoked and have not yet expired, its distribution causes network overhead. Moreover, the CRL size increases dramatically if only a small portion of the OBUs in the VANET is revoked. To have an idea of how big the CRL size can be, consider the case where 1% of the total number of the OBUs in the United States is revoked. Recall that in a VANET, each vehicle owes not only an identity certificate, but also several pseudonyms. The number of pseudonyms may vary depending on the degree of privacy and anonymity that it must be guaranteed. According to [5], OBUs must store enough pseudonyms to change pseudonyms about every minute while driving. This equates to about 43,800 pseudonyms per year for an average of two hours of driving per day. In the US, 255,917,664 "highway" registered vehicles were counted in 2008, of which 137,079,843 passenger cars [6]. In this case, the CRL would contain around 100 billion revoked certificates. Assuming that certificates can be identified by a 16 byte fingerprint (the size of one AES block), the CRL size is around 1,7 TB. Only the amount of memory necessary to storage this CRL makes it impossible its deployment.

The CRL size can be reduced by using regional CAs. However, there appears a a trade-off between the size of the CA region and size of the CRL, as well as the management complexity of the entire PKI system for VANETs. The least complicated region to manage would be a single large area, such as the entire United States, with a single CA responsible for every certificate and pseudonym. However, this gives place to CRLs of several terabytes. Therefore, it is necessary to divide the CRL information according to regional areas. In this sense, if we divide the entire United States by cities (i.e. 10,016 cities according to the U.S. census bureau), the CRL size is reduced to around 170 Mbytes. Using the 802.11a protocol to communicate with RSUs in range, vehicles could have between 10-30 Mbps depending on the vehicle's speed and the road congestion [7]. Therefore, in the best case a vehicle will need more than 45 seconds to download the whole CRL. Under non-congested conditions, any vehicle should be able to contact the infrastructure for more than 45 seconds, and therefore download the CRL. In scenarios where vehicles are not able to keep a permanent link with the infrastructure for this amount of time, techniques such as Bloom filter or Digital Fountain Codes could be use to download the CRL. Therefore, though the problem of having a huge CRL is mitigated by the use of such techniques, the restraints imposed by the distribution affect the freshness of the revocation data.

A direct consequence of this significant time to download a CRL is that a new CRL cannot be issued very often, so its validity period has to be shortened. This validity period directly determines how often a vehicle has to update the revocation data. Therefore, the validity period of the CRL is critical to the bandwidth consumption. Moreover, it appears another trade-off between the freshness of revocation data and the bandwidth consumed by downloading CRLs. Large validity periods will decrease the network overhead at expenses of having outdated revocation data. Small validity periods will increase the network overhead but users will have fresh information about revoked certificates. As CRLs cannot be issued every time there is a new revoked certificate, vehicles will be operating with revocation data that is not comprehensive. Therefore, they will be taking certain risk of trusting a certificate that could be potentially revoked.

III. RAR: Risk Aware Revocation Mechanism

Traditionally, CRLs are issued periodically. *Time-stamps* are a typical way of ensuring freshness. In fact, CRLs always include a couple of time-stamps: the instant at which the CRL was issued (`thisUpdate`) and the instant at which the CRL is scheduled to be issued (`nextUpdate`). For instance, if `nextUpdate-thisUpdate = 1 hour`, this means that CRLs are issued every hour, which is its issuing interval.

The problem in VANETs is that the CRL cannot be issued too frequently in order to avoid an excessive network overhead. Therefore, VANETs can be secured only up to a point. Users inside a VANET have to deal with some insecurity that cannot be destroyed. In this context, one should estimate the level of security in relation to some perceived threat. This insecurity always exists and is inherent in a global-scale public key infrastructure. Moreover, in VANETs this insecurity is even higher not only due to its large scale but also to the CRL distribution restrictions.

In this context, we propose a Risk Aware Revocation (RAR) mechanism to communicate users the risk inherent in the vehicular PKI. RAR can be viewed as revocation scheme to control risk. Traditionally, it is often implicitly assumed that everyone should get the most recent CRL. However, in VANETs it may be not efficient to download the most recent CRL. Instead, users should set recency requirements that will determine how recent a CRL should be. More strict recency requirements have lower risk, but they have higher communication costs. Because risk is application-dependent, different applications and users have different recency requirements. For instance, safety applications must use as fresh revocation information as possible, while other applications as infotainment applications could operate with higher risk.

In the following, we describe the different phases of the RAR mechanism:

1) *Risk calculation*: During this phase the CA calculates the risk of operating with the cached CRL.
2) *Risk transmission*: Periodically, the each regional CA communicates the risk estimation to the corresponding RSU, which in turn broadcasts it to the vehicular nodes.

A. Risk Calculation

As explained in the previous section, users operate with a cached CRL while being valid. In this sense, the CA issues CRL bounded by two time-stamps:

- *thisUpdate.* Instant at which the CRL was publicized.
- *nextUpdate.* Instant at which an updated CRL is expected to be publicized.

Using these two time-stamps users could try to estimate the risk of operating. However, these time-stamps provide users with a poor criterion. Users could calculate the time elapsed since the CRL publication and compare it to the instant when a new CRL update is expected. With this comparison users could get an idea of the freshness of the revocation information but they could not infer the risk of trusting this data. Depending on the revocation rate, the risk after having elapsed some time since the CRL publication will vary. Therefore, to estimate this risk it is not only necessary this elapsed time but also the revocation rate. The revocation rate is known only by the corresponding CA. So it must be the corresponding CA the entity in charge of publicizing the risk at each instant.

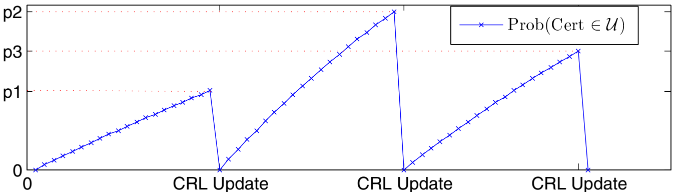

Fig. 1. Time evolution of the probability of considering an unknown revoked certificate as valid.

Using group theory and a basic probabilistic analysis, one can calculate the probability of considering a certificate as a valid one when the real status known by the CA is revoked at time t as (see details in [8]):

$$\rho(t) = Prob(Cert \in \mathcal{U}) = \frac{p(t-t_0)}{(1-p)T_c + p(t-t_0)}, \quad (1)$$

where T_c is the mean certificate lifetime, p is the percentage of revoked certificates and $\mathcal{U}$ is the set of revoked certificates that were not included in the previous CRL.

Figure 1 shows the evolution of $\rho(t)$ during three consecutive CRL updates. As expected, the probability is zero at CRL updates instants as there are no unknown revoked certificates. On the contrary, this probability is maximum just before publicizing a new CRL, as the number of unknown revoked certificates is maximum at this point. Note that this maximum (as well as the slope of the probability function) varies depending of the percentage of revoked certificates (p_i). Thus, when this percentage is higher (note that $p2 > p3 > p1$) the probability increases more rapidly.

Once we have calculated the probability $\rho(t)$, we estimate the consequences of using an unknown revoked certificate to calculate the risk. These consequences will vary depending on the revocation cause of the certificates. The PKIX/X.509 certificate and CRL specification defines nine reason codes for revocation of a public-key certificate (see Table I).

Code	Text Code	w_i	Description
(1)	`keyCompromise`	9	Private key has been compromised
(2)	`cACompromise`	10	CA has been compromised
(3)	`affiliationChanged`	1	Subject's name or other information has changed
(4)	`superseded`	1	Certificate has been superseded
(5)	`cessationOfOperation`	2	Certificate is no longer needed
(6)	`certificateHold`	3	Certificate has been put on hold
(7)	`removeFromCRL`	0	Certificate was on hold and should be removed from the CRL.
(8)	`privilegeWithdrawn`	5	Privileges granted to the subject of the certificate have been withdrawn
(9)	`aACompromise`	10	Attribute authority has been compromised

TABLE I
REVOCATION CODES, WEIGHT VALUES w_i AND DECRIPTION.

Note that we have defined a weight value w_i for each possible revocation cause. This weighting allow us to give more importance to those certificates that were revoked due to a key compromise or malicious use. This weighting is purely intuitive as there are some revocation causes that poses bigger threats than other causes. For instance, the compromise of the CA's private key is more dangerous and has potentially more disastrous consequences than a superseded certificate.

In order to calculate the value of the consequences $Q(t)$, the CA has to calculate the ratio of revoked certificates related to each revocation cause $r_i(t)$ and calculate the weighted mean. Thus, the consequence value $Q(t)$ can be expressed as:

$$Q(t) = \frac{\sum_{i=1}^{9} w_i r_i(t)}{\sum_{i=1}^{9} w_i}. \quad (2)$$

Once the CA has estimated the consequences of operating with the new revoked certificates, it can calculate the risk as:

$$Risk(t) = Q(t) \cdot \rho(t). \quad (3)$$

It is worth noting that this risk will increase over time as the probability of operating with an unknown revoked certificate also increases with time. The risk will be zero when a new CRL is publicized (though there always exists some inherent risk that the CA is not aware of) and it will grow afterwards until every known revoked certificate has expired. At this point, the risk will achieve its maximum as all revoked certificates will be unknown.

B. Transmitting the risk value

The RAR mechanism takes advantage of the physical layer used in VANETS to transmit the risk value to vehicles. The physical layer in VANETS is based in the Dedicated short range communication (DSRC) protocol [9]. DSRC is a 75 MHz band in the 5.9 GHz frequency range with seven non-overlapping channels. Two different channel types are described for use in DSRC. The first type is the control channel, referred to as CCH, which is a single channel reserved for short, high-priority application and system control messages

[3]. During the CCH, every node broadcasts a beacon that provides trajectory and other information about the vehicle. The other type of channel is the service channel, or SCH, which has six different 10 MHz channels that support a wider range of applications and data transfer. During CCH time channel activities on SCH are suspended and vice versa

The RAR mechanism uses the CCH to transmit the risk value of the current public CRL. Each node in the VANET monitors the CCH during time periods designated as control channel intervals. The time period for an entire CCH Interval and SCH Interval is called a Sync Interval. Between CCH intervals, nodes may switch to participate on a SCH for applications such as file downloads.

Each regional CA sends to RSUs an authenticated message M containing the risk value and a time-stamp.

$$CA \rightarrow RSUs : M = [Risk, TimeStamp]_{Sign_{CA}}.$$

Note that regional CAs are expected to have a wireline to communicate with their corresponding RSUs. The time stamp included in the message allows vehicles to verify the freshness of the message and at the same time check at which instant the risk value was calculated. Thus, it is avoided potential forgery or replay attacks. The size of this message is 72 bytes: 64 bytes for the ECDSA-256 CA's signature, 4 bytes for the timestamp representing seconds UTC since the epoch ('1970-01-01 00:00:00'), and 4 bytes for representing the risk value.

During the CCH interval, RSUs broadcast this message to OBUs in range. However, not in every CCH interval M is sent. Depending on the certficate revocation rate, each regional CA will choose the rate at which they have to trasmit the risk to the vehicles. Normmaly, certificates will be revoked at a frequency lower than $100ms$. For instance, if a certificate is revoked every minute, the CA will have to set the risk tranmission rate to one message per minute at most. On the other hand, vehicles that are not in the range of any RSU, can take advantage of V2V communication to request other vehicle for the risk value. Notice that as M is signed by the CA, any vehicle can act as repository and transmit this message without being able to modify it. OBUs check the authenticity and the freshness of the message, otherwise they discard it. Once checked, OBUs are able to know the risk of operating with unknown revoked certificates in the vehicular network. Indirectly, the risk value provides them with an idea of how many revoked certificate are unknown to them. Depending of the recency requirement of the application and the user, they could operate to operate under this risk or contact the RSU to get a fresher CRL.

IV. Evaluation

In this section, the efficiency of the proposed mechanism for transmitting the risk of operating with unknown revoked certificates is verified through simulation using NCTUns [10]. The reference scenario consists of 4 two-lane roads forming a 1000x500m rectangle. Three RSUs are placed every 300 meters. Note that there are some areas of the highway that are not covered. Table II summarizes the values of the configuration parameters used in the reference scenario.

Parameter	Value
Area	1000x500m
Number of RSUs	10
Number of OBUs	100
RSU Transmission range	300m
MAC	IEEE 802.11p

TABLE II
Parameter values for the reference scenario.

First of all, we evalute the overhead introduced by the RAR mechanism. To do so, we configure the RSUs to transmit the risk every second. Figure 2 shows the incoming througput in the CCH channel of a randomly chosen vehicle. As expected, the vehicle is receving messages from the RSU in range every 100 ms; and every second it receives the risk message M that involves an increase of the incoming throughput of 72 bytes. In this sense, the overhead introduced by the RAR mechanism is of 4% in the CCH channel. It is worth noting that in a real VANET scenario this overhead is expected to be lower, as the risk message will not be sent every second. Sending the risk messsage every second represents VANETs with incredibly high revocation rates or VANETS where users have great demands of recency of the revocation information.

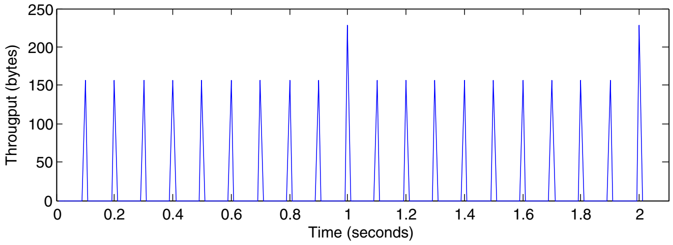

Fig. 2. CCH througput of a randomly chosen vehicle.

Once we have shown that the overhead introduced by the RAR mechanism is low, hereon we show its performance benefits. To that end, we configure three different types of risk users profiles:

- Risk-averse: users that operate iff $Risk(t) \leq 0.3$.
- Risk-neutral: users that operate iff $Risk(t) \in [0.3, 0.5]$.
- Risk-loving: users that operate iff $Risk(t) \leq 0.9$.

We configure each one of the 100 OBUs to follow one of these three profiles. Then, we calculate the risk of operating in the network. As we do not have revocation information of a real vehicular scenario, we use revocation data conatined in a CRL from GoDaddy. Godaddy is the trusted provider of Internet infrastructure services for the networked world that leads the global SSL marketplace.

On the one hand, using this CRL, we obtain number of revoked certificates per day. We use this information to calculate the probability of using a revoked certificate $\rho(t)$. On the othen hand, in order to calculate the consequences Q we obtain the revocation codes of each revoked certificate contained in the CRL. In this context, Figure 3 shows the revocation causes.

This analysis covered more than 300,000 certificates. It is worth noting, that the main cause of revocation is the cessation of operation, i.e., the certificate is no longer needed for its original purpose. The rest of revocation causes are highly improbable compared with the main cause. Using the weights defined in Table I we obtain a value of $Q = 0.12$.

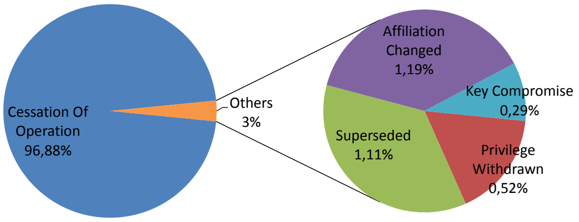

Fig. 3. Revocation causes of code-signing certificates issued by GoDaddy.

Thus we can calculate $Risk(t)$ during seven days. As shown in Figure 4, the risk is zero at the CRL update times (in the case of GoDaddy every 24 hours), and then it grows according to the number of revoked certificates.

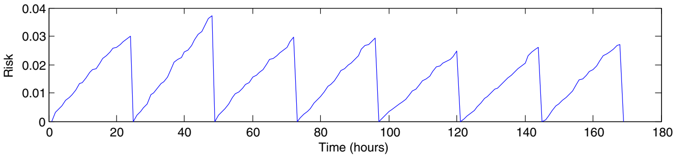

Fig. 4. Risk of using a revoked certificate.

Finally, we run the simulation scenario during 7 days, and we calculate the time during which vehicles are willing to operate. Figure 5 shows the mean time that a vehicle is willing to operate in the network according to each profile. As expected, risk-averse users operate during less time that risk-loving users. Note that the relation between both profiles is not directly proportional, as the risk grows according to the number of revocations. It is also worth noting that due to the lack of coverage in some areas of the network there are some users that operate for longer time than user having the same profile. Due to this same reason, some users are operating in the network even when the risk exceeds its profile because they are not able to download the risk message neither from the RSU nor from another vehicle.

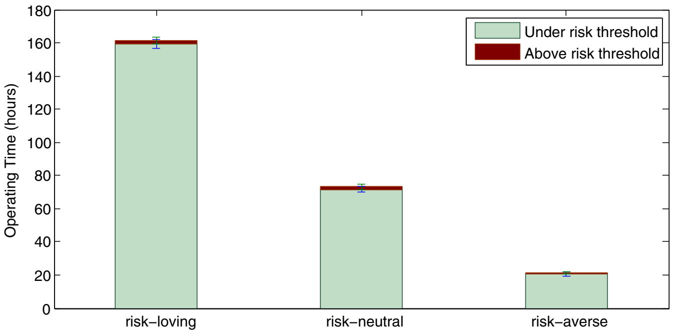

Fig. 5. Operating time for each type of user profile.

V. Conclusions

In this paper, we have analyzed the limits on the adoption of CRLs to manage revocation in Vehicular Ad Hoc Networks (VANETs). We have shown that the adoption of CRLs is feasible in vehicular networks when using regional CAs and techniques to reduce the CRL size and optimize its distribution. However, the freshness of the revocation information contained in the CRL must be managed in order to reduce the overhead introduced in the network by the CRL distribution.

In order to make users aware of the freshness of the revocation information, we have proposed a risk aware revocation (RAR) mechanism. Risk associated with a vehicular PKI cannot be completely removed, but it can be analyzed and controlled. Under RAR, users will receive timely information about the freshness of the CRL they have stored. Hence, users with higher recency requirements lead to lower risk but require higher communication and/or computation cost. RAR provides users with the necessary information to set their recency requirements so that they can balance the risk and the cost. Users should be able to set different recency requirements based on their needs and resources. We have shown that depending on the attitude towards risk of a user, they will able to operate for longer periods of time.

Acknowledgments

This work is funded by the Spanish Ministry of Science and Education under the projects CONSOLIDER-ARES (CSD2007-00004) and TEC2011-26452 ”SERVET“, and by the Government of Catalonia under grant 2009 SGR 1362.

References

[1] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, ser. SASN ’05, 2005, pp. 11–21.

[2] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for secure and private vehicular communications,” in *Telecommunications, 2007. ITST ’07. 7th International Conference on ITS*, Jun. 2007, pp. 1 –6.

[3] “IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages,” *IEEE Std 1609.2-2006*, pp. 1–105, 2006.

[4] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, “Certificate revocation list distribution in vehicular communication systems,” in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, ser. VANET ’08, 2008, pp. 86–87.

[5] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, “Design and analysis of a lightweight certificate revocation mechanism for vanet,” in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, ser. VANET ’09. New York, NY, USA: ACM, 2009, pp. 89–98.

[6] B. of Transportation Statistics U.S. Department of Transportation, “Number of u.s. aircraft, vehicles, vessels, and other conveyances,” http://www.bts.gov/publications/national_transportation_statistics/html/table_01_11.html, 2009, [Online; accessed 31-July-2011].

[7] D. N. Cottingham, I. J. Wassell, and R. K. Harle, “Performance of ieee 802.11a in vehicular contexts,” in *In Proc. IEEE VTC*. Spring, 2007.

[8] J. L. Muñoz, O. Esparza, C. Gañán, and J. Parra-Arnau, “Pkix certificate status in hybrid manets.” in *WISTP*, ser. Lecture Notes in Computer Science, vol. 5746. Springer, 2009, pp. 153–166.

[9] *IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments*, May 2008.

[10] S. Y. Wang and C. L. Chou, “Nctuns tool for wireless vehicular communication network researches,” *Simulation Practice and Theory*, vol. 17, pp. 1211–1226, 2009.