SmartRevoc: An Efficient and Privacy Preserving Revocation System Using Parked Vehicles

David Eckhoff*, Falko Dressler† and Christoph Sommer†
* Computer Networks and Communication Systems, Dept. of Computer Science, University of Erlangen, Germany
† Computer and Communication Systems, Institute of Computer Science, University of Innsbruck, Austria
eckhoff@cs.fau.de, falko.dressler@uibk.ac.at, christoph.sommer@uibk.ac.at

***Abstract*—Security and privacy requirements in vehicular networks are typically addressed using a Public Key Infrastructure (PKI) and pools of pseudonymous certificates for each vehicle. Messages are signed with these certificates, so that misbehaving vehicles can be excluded from the network by disseminating Certificate Revocation Lists (CRLs).**

We present *SmartRevoc*, a novel revocation architecture, to solve the main challenges of CRL distribution in vehicular networks: CRL size, dissemination speed, and preservation of location privacy. Using two hash chains, we compute CRLs on vehicles, substantially reducing communication overhead. At the same time our design is privacy preserving, preventing the linking of past pseudonyms to revoked ones. We additionally utilize parked vehicles to epidemically disseminate CRLs and show that even few parked vehicles can outperform an unreasonably high number of Roadside Units (RSUs). Our simulation results clearly indicate that *SmartRevoc* is a major step forward toward more efficient and secure vehicular networks.

I. Introduction

The wireless exchange of information between vehicles (and infrastructure) can bring numerous benefits for drivers. Besides comfort applications and traffic flow optimization, one of the key objectives of such Intelligent Transportation Systems (ITS) is to improve traffic safety [1]. In order to achieve this, both in terms of technological feasibility and envisioned marked acceptance, two key requirements have to be met:

First, drivers have to be able to trust information obtained through the system, meaning that it must be possible to detect messages forged by an attacker, but also that faulty vehicles can be excluded from participating in the vehicular network [2]. Secondly, the system should neither directly nor indirectly (through weak security mechanisms) disclose private information of its users [3].

Current designs for ITS address these two challenges by the use of a Public Key Infrastructure (PKI) [4]. In order to authenticate messages while still preventing tracking, vehicles sign messages using changing certificates called *pseudonyms*. However, to ensure the proper operation of safety systems, any vehicle that sends false messages (whether maliciously or because of a broken sensor) needs to be excluded from further participation.

This is accomplished by certificate revocation, via the distribution of Certificate Revocation Lists (CRLs). Messages signed with a revoked certificate must be ignored to avoid that false information is given to safety applications.

The faster this revocation process is, the shorter the period of time within an attacker may compromise the system. Thus, a low delay for disseminating new CRLs to participating vehicles is critical to the success of the system.

Depending on the available communication technology, there are different approaches to distributing CRLs: If all vehicles have cellular Internet access, a CRL could easily be pushed to the vehicles, possibly even via multicast mechanisms, reducing the delay to an absolute minimum. However, traffic over cellular networks is not free. Moreover, even though IEEE 802.11p Dedicated Short-Range Communication (DSRC) on-board units are currently envisioned to become mandatory, cellular technology will likely remain optional. Thus, a large portion of vehicles is unlikely to be retrofitted with cellular technology.

Distributing the CRL over a Vehicular Ad Hoc Network (VANET), consisting of vehicles and Roadside Units (RSUs), e.g., using the mentioned DSRC technology, is thus a promising approach; however, this makes both delay and channel load critical properties of this system.

We address the first goal – reducing the channel load incurred by the distribution of CRLs – as follows. Our approach makes use of very small CRLs by employing two hash chains and shifting the task of computing which certificates have been revoked to the vehicles. When used with time slotted pseudonym pools [5], [6], our system provides backward privacy to all users, that is, it ensures the inability of an attacker to retroactively disclose location information about vehicles with revoked pseudonyms. However, in terms of storage and overhead, our system is just as efficient without the use of time slotted pseudonym pools.

We also address the second goal – reducing the delay from initial revocation of a pseudonym to wide area dissemination of a new CRL. Especially in the early stages of an ITS the penetration rate (i.e., the fraction of vehicles equipped with a DSRC unit) will be small and connectivity will thus be low [7]. However, good connectivity of the network is critical for disseminating new CRLs quickly. We propose the use of parked vehicles to increase connectivity and thereby decrease the delay. Parked vehicles have been shown to be able to contribute to road safety, especially in urban environments [8], but also to be beneficial for non-safety applications such as Internet access or information exchange [9]–[11]. We extend their use to also include security related tasks.

978-1-4799-0537-9/13/$31.00 ©2013 IEEE

Based on these findings, we developed *SmartRevoc*, which explicitly addresses the mentioned two goals. In this paper, we outline its architecture, its capabilities, and present comprehensive performance results.

Our contributions can be summarized like this:

- We present *SmartRevoc*, a very efficient revocation system that allows for fast and easy distribution of CRLs.
- To the best of our knowledge, we are the first to make use of parked vehicles for security purposes and show, that by doing so, revocation delays can be substantially decreased.
- Our approach is privacy preserving and prevents the disclosure of location information even for vehicles with revoked certificates.

II. Related Work

The first subject of this paper, the participation of parked vehicles to support different applications of an ITS, has been proposed by several authors [8]–[11].

Liu et al. presented a method to use parked vehicles as relay nodes to disseminate information in a Delay Tolerant Network (DTN) fashion [9]. They mainly focus on connectivity and show that an ITS can greatly benefit from additional nodes. However, they do not provide insights on latency, which is crucial for the revocation of certificates.

In a previous work we investigated [8] communication latency with a special focus on traffic safety, showing that parked vehicles can help improve safety when used as relay nodes and cope with radio shadowing by routing around obstacles in an urban environment. In this paper we now highlight an additional use for parked vehicles, to assist security and privacy in vehicular networks.

Crepaldi et al. [10] as well as Malandrino et al. [11] expand on the discussion of parked cars as relay nodes to further investigate their usefulness; they propose that parked vehicles can be used to share and provide opportunistic Internet access to other vehicles. Subsequently, in [12], they also present an energy management scheme to increase the lifetime of parked vehicles and thus improve the offered service.

The second subject of this paper, certificate (i.e., pseudonym) revocation in vehicular networks, has been widely studied [6], [13]–[17], albeit with different goals.

Lequerica et al. propose the dissemination of CRLs using cellular communication [13]. They show that using multicast mechanisms a CRL can be very quickly distributed. For reasons outlined in Section I we focus on the problem of epidemic dissemination of CRLs using inter-vehicle communication only. Furthermore, we also consider the privacy of users as a feature of the system.

An example of a DSRC-only system is the approach presented by Laberteaux et al. [14]; here, CRLs are injected into the VANET by RSUs and then distributed by all moving vehicles. This work showed that the latency substantially decreases when the network density is very high. We show a possible way to also achieve this in sparse scenarios: by the participation of parked vehicles.

In order to decrease bandwidth usage when disseminating CRLs in an epidemic fashion, Haas et al. [15] propose that only missing pieces of the CRL are exchanged between vehicles. Our approach also makes use of this mechanism by only sending delta updates to nearby nodes instead the full CRL.

Another reduction of the CRL size to increase the efficiency of CRL distribution has been proposed in [16]. The authors recommend splitting the CRL into pieces and to only contain regional revocation information. Even though CRLs are already very small in our approach, this method could be used to further decrease their size.

In [17], the usage of Bloom Filters to lower the computational effort was introduced. Bloom filters offer a probabilistic method to check whether a pseudonym is on a CRL. The reduction of network overhead was discussed in [18], where instead of full lists only deltas are transmitted. *SmartRevoc* uses this method to transmit a CRL once it is discovered that the CRL of another vehicle is not up-to-date.

The work we consider to be the most related to our *SmartRevoc* system has been introduced by Haas et al. in [6]. In contrary to previous schemes, their approach accounts for backward location privacy while using a very efficient revocation method. It extends the certificate for slot r by one field, the certificate identifier $C_i = E_{s_i}(r)$, which is the result of a block cipher E or a Cryptographic Pseudo-Random Number Generator (CPRNG) that uses elements s_i of a hash chain $s_i = h(s_{i-1})$ as its key. When revoking a certificate, s_i and i are published and vehicles can then compute all subsequent $C_j : i \leq j \leq n$.

Our system does not require the use of two different cryptographic functions, but can be based on one cryptographic hash function only, reducing possible security issues, especially when the block cipher is only used with known plaintext, although current ciphers are not believed to be susceptible.

Furthermore, their simulation study was not based on packet-level communication, so the specific radio shadowing characteristics in urban environments were not accounted for.

Finally, the distribution of CRLs was based on moving vehicles and RSUs only.

III. Public Key Infrastructures in Vehicular Networks

The common approach for meeting security and privacy requirements in an ITS is the deployment of a Public Key Infrastructure (PKI) [4]. Both user authorization and message integrity can be reached through the signing of messages with signed certificates, while location privacy is believed to be preserved when the used certificates are frequently changed [3].

A simplified vehicular network PKI is illustrated in Figure 1: Each vehicle v is pre-equipped with a base identity certificate I_v, the private key K_v^-, and the certificate of the central certificate authority I_{CA}. The base certificate I_v is already signed by the authority using the corresponding private key of I_{CA} and is thus the key to entering the network.

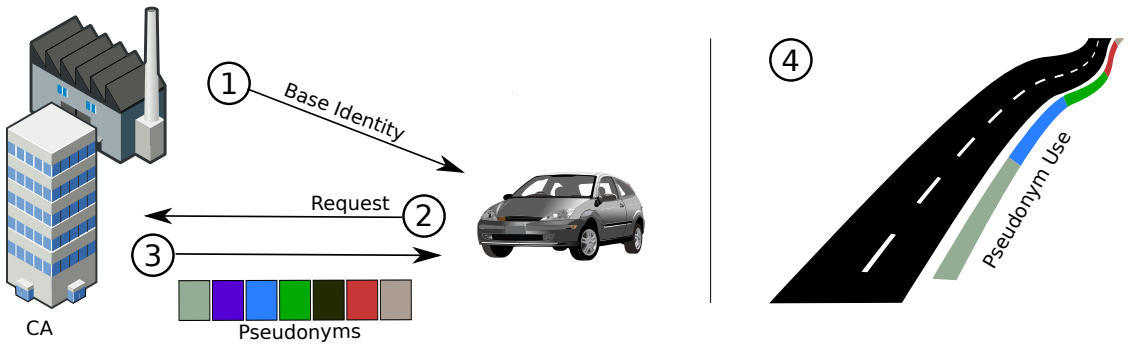


Figure 1. Principles of a PKI in vehicular networks: (1) The vehicle is pre-equipped with a base identity (2) The vehicle requests the signing of pseudonyms (3) The CA signs the pseudonyms if they have been created using the base identity (4) The vehicle uses the pseudonyms as its address.

After the vehicle generates n private/public key pairs along with corresponding certificate signing requests it uses I_v to request the signing of these pseudonym certificates $P_x \in P$ from the CA. The CA checks if this signing request comes from a legitimate vehicle (i.e, I_v is signed) and signs the pseudonyms P_v with private key of I_{CA}.

Once the vehicle has received the pseudonyms it chooses one pseudonym $P_x \in P$ to sign messages. To prevent traceability of vehicles, the used MAC address has to also be altered, e.g., by deriving it from the used pseudonym. A message consists of its information M, the encrypted signature $h(m)$ with private key K_x^-, and the certificate P_x containing the public key K_x^+. A recipient of a message first has to check if P_x was signed by I_{CA} and if it's valid. If so, it computes $h(m)$ and decrypts the signature with K_x^+. If both values are identical the message is valid.

Each vehicle will frequently change its pseudonym to preserve its location privacy. This is possible because only the Certificate Authority (CA) can resolve a pseudonym to a base identity.

While various changing strategies exist in the literature [19], we propose the use of timed-slotted pseudonym pools [5] due to their efficiency and good characteristics when it comes to Sybil attacks [20]. At each arbitrary point in time a vehicle has only one valid pseudonym certificate and changes it when a time-slot has passed. The contrary approach would be that all pseudonyms are always valid and a vehicle can choose an arbitrary pseudonym from its pool – unbounded by time, location, or context. Both approaches can be combined by the use of n time-slotted pools, where vehicles have only n pseudonyms at each arbitrary point of time. Our revocation scheme works with all three approaches, however, it can only preserve backward privacy when used with time-slotted pools.

If a vehicle sends erroneous data (involuntarily or deliberately) it is desirable to exclude this particular vehicle from the network. Revocation might also be needed when a vehicle changes ownership [6]. This can be done through revocation of all its valid pseudonyms, invalidating messages signed with these pseudonyms. The sooner a vehicle is informed of a new Certificate Revocation List (CRL) the smaller the possible damage by erroneous data is.

Listing pseudonyms on a CRL, however, makes it possible to link them to each other and is therefore a privacy critical process. Backward privacy of a vehicle with revoked certificates should be preserved, i.e, the CRL must not be used to disclose past locations or tracks of a vehicle.

Depending on the pseudonym pool size, the number of pseudonyms that have to be revoked can get considerably big. A faulty software or sensor component in a certain make or model of vehicle could require that the certificates of a large number of vehicles need to be revoked. It is thus important to use an efficient revocation scheme in which CRLs can be quickly exchanged.

As can be seen, efficiency, latency, and privacy are challenging tasks when it comes to revoking pseudonyms. We will show that our approach, *SmartRevoc*, successfully contributes to solving these issues.

IV. The Use of Parked Cars in Vehicular Networks

In the first years of ITS deployment, the number of vehicles equipped with on-board units (and, thus, the amount of neighbors with which a vehicle can communicate) will be low [7]. Combined with the fact that – on average – a vehicle is parked for 23 hours a day [21] and only moving vehicles are exchanging information, connectivity will be a major issue.

A 2003 study of parking behavior in the area of Montreal [22] showed, that only 3.7 % of parked vehicles are parked in interior parking facilities. With almost 70 % of all parked cars being parked on streets the amount of possible communication partners would significantly increase if parked vehicles participated in an ITS. The study furthermore showed that these parked vehicles are widely distributed throughout the whole city, enabling them to increase connectivity not only at certain high density spots but also, or even especially, in low-density areas.

Widespread availability of DSRC radio equipped cars can be predicted: currently, the U.S. Department of Transportation (US DOT) is evaluating DSRC deployment in its Connected Vehicle Safety Pilot Program. This study is envisioned to jumpstart commercialization in the automotive and consumer electronics [23].

A. Possible Applications

The applications for the participation of parked vehicles in VANETs are manyfold: It has been proposed to use parked cars as relay nodes for moving vehicles to help deliver non-safety related information in a DTN fashion [9]. Another non-safety approach is the utilization of parkers along the street to provide vehicular internet access [10]–[12].

However, we believe that one of the most important goals of Inter-Vehicle Communication (IVC) is the improvement of traffic safety. Especially in urban environments, radio shadowing caused by obstacles such as buildings or vehicles is a major issue; we were able to show that a potential solution is the use of parked vehicles as relay nodes [8]. These vehicles can route *around* obstacles and give drivers valuable extra seconds to react to certain traffic conditions.

Parked cars have also been shown to increase safety or provide comfort applications, but to the best of our knowledge we are the first to propose their use for the dissemination of CRLs to support security and privacy applications.

B. Energy Management

While moving vehicles seem to have a virtually unlimited amount of energy for the operation of an On-Board Unit (OBU) this is clearly not the case for their parking counterparts. The system must never drain the battery of the vehicle below a point where ignition or the operation of mandatory functions is no longer possible.

Basically, there are two approaches to overcome this problem: Either the OBU has a dedicated battery that is also recharged when the vehicle moves, or the OBU knows about the current battery level and can then switch itself off according to a threshold.

As a complete energy management scheme is out of scope for this paper we investigated the energy needed for the operation of a radio: A typical IEEE 802.11p OBU does not drain more than 1 W on average (this is a generous upper limit based on specifications of early prototypes; regular OBUs are expected to drain less). The battery of a small vehicle provides about 480 Wh to 840 Wh [24], thus allowing the OBU to run for 20 days. Even if the maximum allowed drainage for the OBU is set to 10 % when the vehicle is parked, the system can still run for 2 days.

An energy management scheme has been presented in [12]. It provides near-optimal energy efficiency when the stop duration can be estimated perfectly, but is also capable of reacting to random errors, further increasing the time an OBU can operate when the vehicle is parked.

In conclusion, we can say that the participation of parked vehicles in a VANET is not critical when the parking time is less than one day. This becomes even less of an issue with bigger, hybrid, or electric vehicles. For example, a Tesla Roadster with its 53 000 Wh battery capacity could theoretically operate an OBU for several years. For the remainder of this paper we assume that, without loss of generality, all parked vehicles always have sufficient energy to operate the DSRC OBU.

V. SmartRevoc

In order to revoke whole sets of certificates without transmitting the complete set, the CA includes an additional identifier C_i in each certificate. The CA generates and stores a secret key ρ_v for each vehicle v (refer to Table I for a quick reference of symbols we introduced in the following).

To demonstrate the need for the design we propose, let us first assume that the CA uses a known, keyed cryptographic hash function $h(\,\cdot\,,\,\rho_v)$ to generate a set of related identifiers $C_1, \ldots, C_i, C_{i+1}, \ldots, C_N$ as

$$\begin{aligned} C_1 &= \text{rand()} \\ C_{i+1} &= h(C_i,\,\rho_v) = h(C_1,\,\rho_v)^{(i)} \end{aligned} \tag{1}$$

This leads to a hash chain of identifiers

$$C_1 \xrightarrow[h(C_1,\,\rho_v)]{} C_2 \xrightarrow[h(C_2,\,\rho_v)]{} C_3 \xrightarrow[h(C_3,\,\rho_v)]{} \cdots \tag{2}$$

A CRL entry to revoke all n certificates after C_i (typically $n = N - i$ to completely revoke the pool of N certificates) would be:

$$\text{CRL}_{(v,i)} = (C_i,\,\rho_v,\,n) \tag{3}$$

However, this allows an attacker to run a brute force attack of complexity $N - n$ to reveal any observed past identifier C_j as belonging to the same set as a currently revoked C_i by executing Algorithm 1 on $\text{CRL}_{(v,i)}$.

Thus, when a match is found, not just the current and future privacy of vehicle v is disclosed, but also part of its past privacy (i.e., its identity during the time between using C_j and the publication of the CRL).

Algorithm 1 Attack to reveal whether any C_j is a past identifier of a pseudonym revoked in $\text{CRL}_{(v,i)}$

Require: $C_j,\ \text{CRL}_{(v,i)} = (C_i,\,\rho_v,\,n),\ N$
1: **for each** $m \in [1, N-n]$ **do**
2: **if** $h(C_j,\,\rho_v)^{(m)} = C_i$ **then**
3: **return true** ▷ C_j is a past identifier of C_i
4: **end if**
5: **end for**
6: **return false** ▷ C_j is not a past identifier of C_i

Table I
Overview of symbols used in this paper

Symbol	Meaning
N	Size of certificate pool
C_i	Identifier of certificate i
$\text{CRL}_{(v,i)}$	CRL for vehicle v, starting with certificate i
$h(\,\cdot\,,\,k)$	Keyed cryptographic hash function, using key k
$h(\,\cdot\,,\,k)^{(i)}$	$h(\,\cdot\,,\,k)$ applied to its own result i times
$s(\,\cdot\,)$	Cryptographic hash function
ρ_v	Key for vehicle v stored at CA
ρ_v^i	Key for vehicle v, hashed $i-1$ times using $s(\,\cdot\,)$
P	Pseudonym pool of a vehicle

Our *SmartRevoc* scheme therefore makes use of a second, un-keyed[1] cryptographic hash function $s(\cdot)$. This function is used to construct a new secret ρ_v^i for each step of generating C_i, yielding

$$\begin{aligned} \rho_v^1 &= \rho_v & C_1 &= \text{rand}() \\ \rho_v^{i+1} &= s(\rho_v^i) & C_{i+1} &= h(C_i,\, \rho_v^{i+1}) \end{aligned} \tag{4}$$

This results in two hash chains:

$$\begin{array}{ccccccccc} \rho_v & \xrightarrow{s(\cdot)} & \rho_v^2 & \xrightarrow{s(\cdot)} & \rho_v^3 & \xrightarrow{s(\cdot)} & \cdots & & \\ & & \downarrow & & \downarrow & & & & \\ C_1 & \xrightarrow[h(\cdot,\cdot)]{} & C_2 & \xrightarrow[h(\cdot,\cdot)]{} & C_3 & \xrightarrow[h(\cdot,\cdot)]{} & \cdots & & \end{array} \tag{5}$$

A CRL entry to revoke all n certificates after C_i would now look like:

$$\text{CRL}_{(v,i)} = \big(C_i,\, \rho_v^i,\, n\big) \tag{6}$$

In order to execute a similar brute-force attack as shown before, an attacker now needs to know either ρ_v (which is never disclosed) or ρ_v^j to start from C_j. However, it is not possible to compute ρ_v^{i-1} from ρ_v^i due to the nature of the cryptographic hash function s.

A. Overhead for Storage

Our approach requires certificates to be extended by only one field, the certificate identifier C_i, which is the output of a cryptographic hash function, such as the SHA-256. A typical [6] size for this value would be 16 B. Depending on the size of the pseudonym pools and the resulting hash collision probability, a longer or smaller value can be chosen, either by truncating the hash-output or by using a hash function with a longer output. Assuming one pseudonym is valid for 600 s [5], [6] and pseudonyms are not re-used, a vehicle needs to store 52 560 pseudonym certificates for one year. Thus, *SmartRevoc* will require an additional 800 kB of storage space on the vehicle.

The certificate authority only needs to store an additional p_v for each participating vehicle v, resulting in an overheard of 16 B per vehicle. The probability of hash collisions, that is, two pseudonyms having the same certificate identifier, depends on the size of C_i. As an alternative, if hash collisions must be completely avoided, the CA could save all issued certificate identifiers, checking against collisions before signing pseudonyms, and, in case of a collision, choose a different p_v.

B. Overhead for Messaging

To reduce message overhead, the currently known CRL version is piggybacked on periodic safety beacon messages; these are commonly envisioned to be sent with a frequency of 10 Hz [25]. The CRL version can be an integer of 4 B and is only attached to a beacon message once every second, resulting in an negligible overhead of 4 B/s per vehicle.

[1]For ease of implementation, the same $h(\cdot,\cdot)$ can be used with a fixed dummy key to supply $s(\cdot)$.

C. Overhead for CRL Distribution

When used with 16 B identifiers a *SmartRevoc* CRL uses 36 B for one revoked vehicle, consisting of C_i = 16 B, p_v^i = 16 B and n = 4 B. Considering certificate overhead (every update of the CRL has to be signed by the certificate authority), more than 30 vehicles can be revoked within one packet.

The CRL is injected by RSUs (or possibly a vehicle with cellular internet access) and then distributed in an epidemic fashion using both moving and parking vehicles.

When a node detects that his own version of the CRL is higher than the one piggybacked in a safety beacon received from another vehicle it will try to broadcast the delta of the CRL. However, to keep channel load and packet collisions low, vehicles do not broadcast CRL updates immediately to avoid triggering what is commonly known as a broadcast storm. Instead, similar to common broadcast suppression schemes [26], CRL broadcasts are delayed by a random time (up to 1 s and 10 s for moving and parking vehicles, respectively). The broadcast will only be performed if, during this time, no other vehicle broadcasts a CRL.

VI. Simulation Study

In addition to the analytic study to show the correctness of our approach we investigated the behavior and effects of our CRL distribution scheme in an extensive simulation study. For this, we used Veins 2.0 [27], an Open Source vehicular network simulator[2], which bidirectionally couples the road traffic simulator SUMO and the network simulator OMNeT++. It builds on the MiXiM physical layer simulation framework to provide a rich set of simulation models for realistic simulation of IVC protocols and applications. Radio propagation calculations make use of an obstacle model [28] to accurately model signal attenuation by buildings in a computationally efficient way. Physical and MAC layer simulation employs a fully-featured IEEE 802.11p model [29], configured to represent a single radio / single channel DSRC system. The application layer, piggybacking CRL identifiers on messages and disseminating new CRLs, is implemented as described in Sections V-B and V-C. A summary of all relevant configuration parameters is given in Table II.

We simulated two different scenarios, illustrated in Figure 2. The first scenario, *Ingolstadt*, represents a suburban setting.

[2]http://veins.car2x.org/

Table II
Simulation parameters used in the evaluation.

Parameter	Value
Frequency	5.89 GHz
Channel bandwidth	10 MHz
Bit rate	18 Mbit/s
Transmit power	20 mW
Sensitivity	–92 dBm
Building shadowing parameters β, γ	9 dB, 0.4 dB/m
Equipped Vehicle density	$\approx$ 7, 15, 30 per km^2
Road traffic simulator time step	200 ms

(a) 4 km × 4 km region of Ingolstadt

(b) 4 km × 8 km Manhattan Grid

Figure 2. Regions of interest – the parts of the road traffic simulation scenarios used in the network simulation – for the Ingolstadt and Manhattan Grid scenarios.

The second scenario, *Manhattan Grid*, represents a synthetic city scenario with very high signal shadowing caused by huge building blocks.

The Ingolstadt scenario is based on real geodata of the city of Ingolstadt, Germany. It was designed by importing road and building geometry, speed limits, right of way, one way streets, etc. from OpenStreetMap. We further adapted this data to reflect realistic intersection management (correct turning lanes, coherent traffic light phases). Based on satellite data, we also added parking areas and distributed parking vehicles corresponding to the size of the area. Finally, following the reasoning of Section IV, we also distributed parked cars alongside streets.

The Manhattan Grid scenario is based on regularly spaced vertical and horizontal two-way streets forming 270 m long and 80 m wide blocks, inspired by downtown Manhattan. We modeled the blocks as homogeneous obstacles, randomly distributing parking vehicles on the curbside around them. No dedicated parking areas were considered in this synthetic scenario.

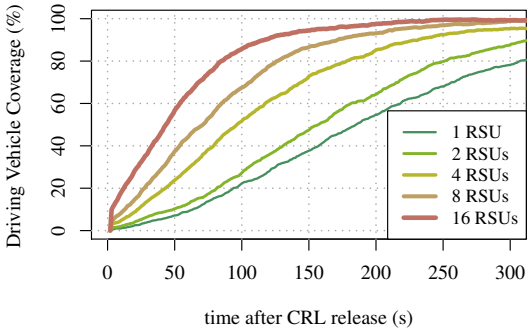
According to [30] different penetration rates can be completely characterized by simulating different traffic densities; Traffic densities were therefore chosen to reflect an early stage of an ITS deployment, where a penetration rate of higher than 10 % cannot be assumed after one year of operation [7]. Each scenario was simulated with low, medium, and high traffic density considering a 10 % penetration rate.

To provide optimal conditions for message dissemination via RSUs we place them at the exact center of intersections. This way transmission ranges could be maximized as signal shadowing caused by buildings had lesser impact.

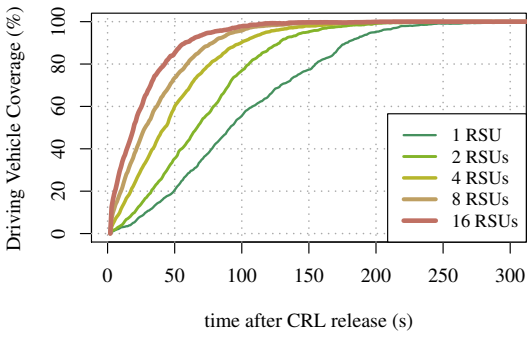
In order to obtain statistically sound results we performed 30 (differently seeded) repetitions of each simulation scenario and parameter set.

A. Time Evolution of CRL Coverage

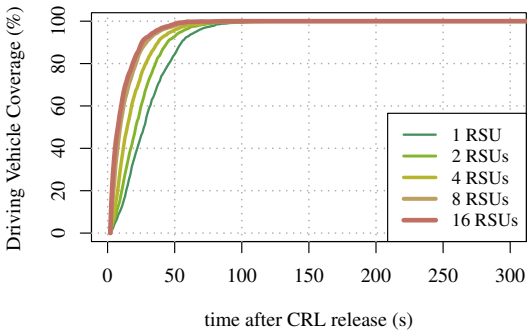
As a first step toward a performance comparison of different penetration rates of parked cars and/or RSUs, we trigger a new CRL to be released at an arbitrary point in time into the simulation (labeled $t = 0\,\mathrm{s}$) and investigate how the CRL coverage, that is the ratio of driving vehicles with the most recent version of the CRL, changes as time progresses. We illustrate the results for the Manhattan Grid scenario and different densities of parking vehicles in Figures 3a to 3c. Distribution in the Ingolstadt scenario behaved similarly, but was noticeably faster because of less pronounced signal shadowing effects.



(a) no parking vehicles

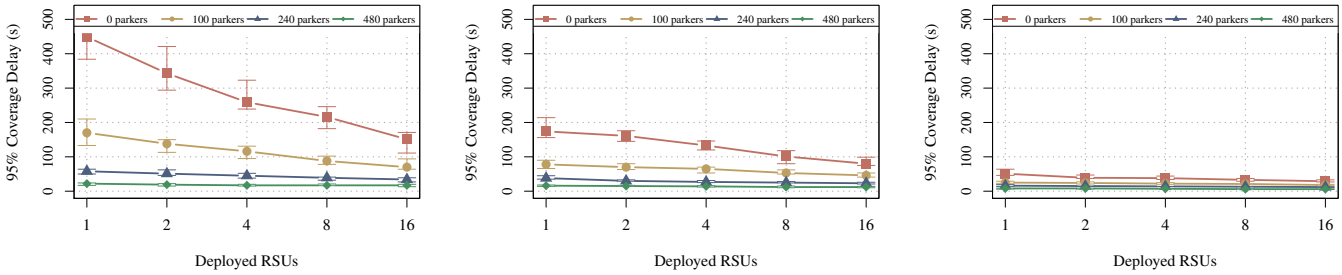


(b) 3.125 parking vehicles per km^2

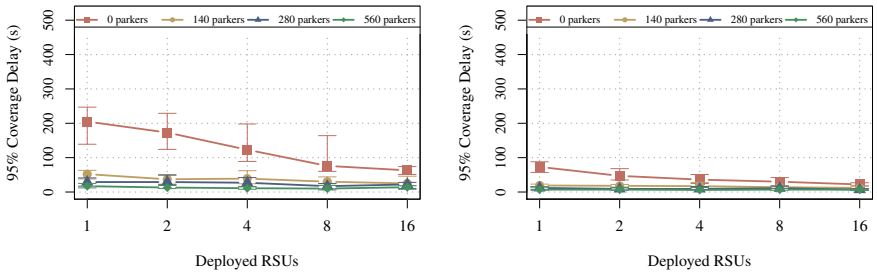


(c) 7.5 parking vehicles per km^2

Figure 3. Evolution of CRL coverage as time progresses in the low traffic density Manhattan Grid scenario, depending on the number of RSUs deployed for CRL injection and the number of parking vehicles available for supporting CRL dissemination.



(a) Manhattan Grid, Low traffic density (b) Manhattan Grid, Medium traffic density (c) Manhattan Grid, High traffic density



(d) Ingolstadt, Low traffic density (e) Ingolstadt, High traffic density

Figure 4. Delay until 95% coverage in the Manhattan Grid and Ingolstadt scenarios with different traffic densities. Parking vehicles help reduce the latency substantially.

Figure 3a shows the impact of employing between 1 and 16 RSUs for injecting new CRLs into the system if no parked cars can be used for disseminating the CRL further. The plots reveal that, without parked vehicles, even an unreasonably large number of RSUs will not be enough for timely CRL dissemination: even reaching just 50 % of vehicles takes on the order of minutes. Figure 3b illustrates how even a small number of parked vehicles, together with a tolerable number of RSUs, can bring median delays down to below one minute. Figure 3c furthermore reveals the minimal impact that increasing the number of RSUs would have in a system supported by 7.5 parking vehicles per km^2, with little difference between deploying as many as 16 and as few as only a single RSU in the whole scenario.

The plots also reveal that CRL coverage increases smoothly, with no sudden jumps or discontinuities. This motivates us to choose the delay it took to reach 95 % CRL coverage as the primary metric for the following comparisons.

B. Delay Until Reaching 95 % CRL Coverage

Figures 4a to 4e illustrate how this metric changes with traffic density and the number of deployed RSUs, depending on the number of available parked vehicles. Error bars show the associated standard deviation of this metric over all simulation repetitions.

In the Manhattan Grid scenario – which is dominated by huge building blocks and thereby strong signal shadowing – the benefit of parking cars to disseminate CRLs is clearly visible, when looking at low traffic (or penetration rate) densities (Figure 4a). The latency of previous approaches (red line, zero parkers) is considerably higher even with 8 deployed RSUs. Adding just as many parking vehicles as driving ones, delays could be more than halved, substantially reducing the need for more than 1 RSU. Even better results were achieved when further increasing the number of parked vehicles, almost establishing full connectivity of the vehicular network.

A higher traffic density (Figure 4b) lowered the absolute benefit of parked vehicles support, but still shows a substantial improvement in terms of latency. In our highest density setup (Figure 4c) network connectivity was already at a level that resulted in low latency. Adding parked vehicles helped improve the situation even more, while additional RSUs only had negligible impact. This means that as soon as the CRL was injected into the network, no additional effort of the provider has to be undertaken to disseminate the CRL with low delay.

Delays in the Ingolstadt scenario were lower because less vehicles were needed to reach high network connectivity. This is due to the lower impact of signal shadowing caused by buildings in this suburban scenario. Nevertheless, Figure 4d shows that a realistic number of parking vehicles equipped with OBUs reduced the update latency well below what could be reached with RSUs only – even when deployed in what we believe to be an unreasonably high number for such a suburban area. In Figures 4d to 4e we observe that the saturation point was indeed reached earlier than in the Manhattan Grid scenario but the results clearly show how a vehicular network can benefit from the help of parked vehicles, especially in the early stages of deployment.

VII. Conclusion and future work

In this paper we presented *SmartRevoc*, an efficient and privacy preserving revocation system. Our system does not require cellular communication but disseminates Certificate Revocation Lists (CRLs) in an epidemic fashion using Dedicated Short-Range Communication (DSRC) technology. Especially in the early stages of an Intelligent Transportation System (ITS) or in low traffic density areas network connectivity can be low, and thus the delay until all vehicles are provided with the latest update of a CRL can be high. We therefore propose the use of parked vehicles which, in comparison to Roadside Units (RSUs), are readily available and basically for free. We show that the update latency could be more than halved in both simulated scenarios, that is Manhattan Grid and the city of Ingolstadt, Germany. In terms of coverage, a reasonable number of parked vehicles could outperform a comparatively high number of strategically well placed RSUs

Our system preserves backward location privacy of drivers, i.e., when a vehicle is revoked linking past pseudonyms is not possible as only future pseudonyms are affected. Through the usage of two hash chains the resulting size of one Certificate Revocation List (CRL) entry to revoke a vehicle's complete pseudonym pool is merely 36 B, while introducing only small overhead in terms of storage and communication.

Future work includes the investigation of larger areas and the impact of equipping only a few vehicles with cellular communication abilities.

References

[1] S. Biswas and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Communications Magazine*, vol. 44, no. 1, pp. 74–82, January 2006.

[2] N. Bissmeyer, C. Stresing, and K. M. Bayarou, "Intrusion Detection in Vanets Through Verification of Vehicle Movement Data," in *2nd IEEE Vehicular Networking Conference (VNC 2010)*. Jersey City, NJ: IEEE, December 2010, pp. 166–173.

[3] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks," in *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*, vol. LNCS 3856. Cavtat, Croatia: Springer, May 2005, pp. 197–209.

[4] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," in *European Wireless 2002*, Florence, Italy, February 2002.

[5] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "SlotSwap: Strong and Affordable Location Privacy in Intelligent Transportation Systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, November 2011.

[6] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient Certificate Revocation List Organization and Distribution," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 595–604, March 2011.

[7] F. Bai and B. Krishnamachari, "Spatio-temporal variations of vehicle traffic in VANETs: facts and implications," in *6th ACM International Workshop on Vehicular Inter-Networking (VANET 2009)*. Beijing, China: ACM, September 2009, pp. 43–52.

[8] D. Eckhoff, C. Sommer, R. German, and F. Dressler, "Cooperative Awareness At Low Vehicle Densities: How Parked Cars Can Help See Through Buildings," in *IEEE Global Telecommunications Conference (GLOBECOM 2011)*. Houston, TX: IEEE, December 2011.

[9] N. Liu, M. Liu, W. Lou, G. Chen, and J. Cao, "PVA in VANETs: Stopped cars are not silent," in *30th IEEE Conference on Computer Communications (INFOCOM 2011), Mini-Conference*. Shanghai, China: IEEE, April 2011, pp. 431–435.

[10] R. Crepaldi, R. Beavers, B. Ehrat, M. Jaeger, S. Biersteker, and R. Kravets, "LoadingZones: Leveraging Street Parking to Enable Vehicular Internet Access," in *Seventh ACM International Workshop on Challenged Networks - CHANTS '12*, Istanbul, Turkey, August 2012.

[11] F. Malandrino, C. E. Casetti, C.-F. Chiasserini, C. Sommer, and F. Dressler, "Content Downloading in Vehicular Networks: Bringing Parked Cars Into the Picture," in *23rd IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2012)*. Sydney, Australia: IEEE, September 2012, pp. 1534–1539.

[12] R. Crepaldi and R. Kravets, "Governing Energy for Parked Cars," in *10th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2013)*. Banff, AB, Canada: IEEE, March 2013, pp. 87–94.

[13] I. Lequerica, J. Martinez, and P. Ruiz, "Efficient Certificate Revocation in Vehicular Networks using NGN Capabilities," in *72nd IEEE Vehicular Technology Conference Fall (VTC2010-Fall)*. Ottawa, Canada: IEEE, September 2010, pp. 1–5.

[14] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in *5th ACM International Workshop on Vehicular Inter-Networking (VANET 2008)*. San Francisco, CA, USA: ACM, September 2008, pp. 88–89.

[15] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET," in *6th ACM International Workshop on Vehicular Inter-Networking (VANET 2009)*. Beijing, China: ACM, September 2009, pp. 89–98.

[16] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems," in *5th ACM International Workshop on Vehicular Inter-Networking (VANET 2008)*. San Francisco, CA, USA: ACM, September 2008, pp. 86–87.

[17] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 8, pp. 1557–1568, October 2007.

[18] D. Cooper, "A More Efficient Use of Delta-CRLs," in *IEEE Symposium on Security and Privacy (S&P 2000)*. Oakland, California, USA: IEEE, May 2000, pp. 190–202.

[19] B. Chaurasia and S. Verma, "Maximizing anonymity of a vehicle through pseudonym updation," in *4th International Conference on Wireless Internet (WICON 2008)*, Maui, HI, November 2008.

[20] J. Douceur, "The sybil attack," in *Peer-To-Peer Systems: First International Workshop*, Cambridge, MA, March 2002, p. 251.

[21] T. Litman, "Parking management: strategies, evaluation and planning," *Victoria Transport Policy Institute*, vol. 25, 2006.

[22] C. Morency and M. Trépanier, "Characterizing Parking Spaces Using Travel Survey Data," CIRRELT, TR 2008-15, May 2008.

[23] U.S. Department of Transportation. Safety Pilot Program Overview and Fact Sheet. [Online]. Available: http://www.its.dot.gov/safety_pilot/

[24] V. Badescu, "Dynamic model of a complex system including PV cells, electric battery, electrical motor and water pump," *Elsevier Energy*, vol. 28, no. 12, pp. 1165–1181, October 2003.

[25] "Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part," ETSI, TS 102 687 V1.1.1, July 2011.

[26] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 84–94, December 2007.

[27] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[28] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A Computationally Inexpensive Empirical Model of IEEE 802.11p Radio Shadowing in Urban Environments," in *8th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2011)*. Bardonecchia, Italy: IEEE, January 2011, pp. 84–90.

[29] D. Eckhoff, C. Sommer, and F. Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," in *75th IEEE Vehicular Technology Conference (VTC2012-Spring)*. Yokohama, Japan: IEEE, May 2012, pp. 1–5.

[30] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in Sparse Vehicular Ad Hoc Wireless Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 8, pp. 1538–1556, October 2007.