Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs

Mohammad Khodaei
Networked Systems Security Group
Stockholm, Sweden
khodaei@kth.se

Panos Papadimitratos
Networked Systems Security Group
Stockholm, Sweden
papadim@kth.se

ABSTRACT

In spite of progress in securing Vehicular Communication (VC) systems, there is no consensus on how to distribute Certificate Revocation Lists (CRLs). The main challenges lie exactly in (i) crafting an efficient and timely distribution of CRLs for numerous anonymous credentials, *pseudonyms*, (ii) maintaining strong privacy for vehicles prior to revocation events, even with *honest-but-curious* system entities, (iii) and catering to computation and communication constraints of on-board units with intermittent connectivity to the infrastructure. Relying on peers to distribute the CRLs is a double-edged sword: *abusive peers* could ''pollute'' the process, thus degrading the timely CRLs distribution. In this paper, we propose a *vehicle-centric* solution that addresses all these challenges and thus closes a gap in the literature. Our scheme radically reduces CRL distribution overhead: each vehicle receives CRLs corresponding only to its region of operation and its actual trip duration. Moreover, a ''fingerprint'' of CRL 'pieces' is attached to a subset of (verifiable) pseudonyms for fast CRL 'piece' validation (while mitigating resource depletion attacks abusing the CRL distribution). Our experimental evaluation shows that our scheme is efficient, scalable, dependable, and practical: with no more than 25 KB/s of traffic load, the latest CRL can be delivered to 95% of the vehicles in a region (50×50 KM) within 15s, i.e., more than 40 times faster than the state-of-the-art. Overall, our scheme is a comprehensive solution that complements standards and can catalyze the deployment of secure and privacy-protecting VC systems.

CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**; **Security protocols**; **Mobile and wireless security**;

KEYWORDS

Vehicular Communications, VPKI, Revocation, CRL Distribution

1 INTRODUCTION

Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications seek to enhance transportation safety and efficiency. It has been well-understood that Vehicular Communication (VC) systems are vulnerable to attacks and that the privacy of their users is at stake. As a result, security and privacy solutions have been developed by standardization bodies (IEEE 1609.2 WG [10] and ETSI [26]), harmonization efforts (C2C-CC [54]), and projects (SeVeCom [66], PRESERVE [69], and CAMP [79]). A consensus towards using Public Key Cryptography (PKC) to protect V2V/V2I (V2X) communication is reached: a set of Certification Authorities (CAs) constitutes the Vehicular Public-Key Infrastructure (VPKI), providing multiple anonymous credentials, termed *pseudonyms*, to legitimate vehicles. Vehicles switch from one pseudonym to a non-previously used one towards unlinkability of digitally signed messages, and improved sender privacy for V2V/V2I messages. Pseudonymity is conditional in the sense that the corresponding long-term vehicle identity (Long Term Certificate (LTC)) can be retrieved by the VPKI entities if deviating from system policies.

In fact, vehicles can be compromised or faulty and disseminate erroneous information across the V2X network [64, 70]. They should be held *accountable* for such actions and credentials (their LTCs and their pseudonyms) can be revoked. To efficiently revoke a set of pseudonyms, one can disclose a single entry for all (revoked) pseudonyms of the vehicle [29, 38, 49, 76]. However, upon a revocation event, all non-revoked (but expired) pseudonyms belonging to the ''misbehaving'' vehicle would also be linked. Linking pseudonyms with lifetimes prior to a revocation event implies that all the corresponding digitally signed messages will be trivially linked. Even if revocation is justified, this does not imply that a user *''deserves''* to abolish privacy prior to the revocation event. Avoiding such a situation, i.e., achieving *perfect-forward-privacy*, can be guaranteed if the VPKI entities are *fully-trustworthy* [39]. However, we need to guarantee strong user privacy even in the presence of *honest-but-curious* VPKI entity; recent revelations of mass surveillance, e.g., [25, 37], show that assuming service providers are fully-trustworthy is no longer a viable approach.

A main concern, relevant to all proposals in the literature [38, 39, 49, 61, 62, 67] is efficiency and scalability, essentially low communication and computation overhead even as system dimension grows. Consider first typical operational constraints: the average daily commute time is less than an hour (on average 29.2 miles and 46 minutes per day) [2, 4, 79] while the latencies for the dissemination of a full Certificate Revocation List (CRL) can exceed the actual trip duration [1]. One can compress CRL using a Bloom Filter (BF) [70, 71, 73]; however, the size of a CRL grows linearly with the number of revoked pseudonyms, thus necessitates larger BFs. More so, a sizable portion of the CRL information is irrelevant to a receiving vehicle and can be left unused. This, at the system level, constitutes waste of computation, communication (bandwidth), and storage resources. In turn, it leads to higher latency for all vehicles to reconstruct the CRL, i.e., a degradation of timely distribution.

Alternatively, vehicles can only validate revocation status of (their neighbors') pseudonyms through an Online Certificate Status Protocol (OCSP) [59]. Even if a VPKI system can comfortably handle such a demanding load [44], OCSP cannot be used as a standalone solution in VC systems: it requires continuous connectivity and significant bandwidth dedicated to revocation traffic, thus impractical due to the network volatility and scale [70]. Moreover, what would be the course of action if the VPKI were not reachable for other reasons, e.g., during a Denial of Service (DoS) attack? So, the challenge is *how can one distribute the most relevant revocation information to a given vehicle, per trip, and ensure timely revocation even without uninterrupted connectivity to the VPKI?*

The computation overhead for the verification of the CRL could interfere with safety- and time-critical operations especially if one considers typical VC rates of 10 safety beacons per second, and thus processing of possibly hundreds of messages from neighboring vehicles per second. Simply put, with existing computation and communication overhead and given the time critical nature of safety applications in VC systems, minimizing the overhead for CRL verification and distribution is paramount.

From a different viewpoint, we need to allocate as little bandwidth as possible for the CRL distribution in order not to interfere with safety critical operations or enable an attacker to broadcast a fake CRL at a high rate. However, this should be hand in hand with timely CRL distribution. This can be achieved with the use of Roadside Units (RSUs) [67]; however, dense deployment of RSUs in a large-scale environment is costly. If the deployment is sparse, a significant delay could be introduced. Alternatively, the CRL can be distributed in a peer-to-peer, epidemic manner [38, 39, 49]. This is a double-edged sword: *abusive peers*, seeking to compromise the trustworthiness of the system, could pollute the CRL distribution and mount a clogging DoS attack.

Despite the plethora of research efforts, none addresses all challenges at hand. In this paper, we show how to *efficiently revoke a very large volume of pseudonyms while providing strong user privacy protection, even in the presence of honest-but-curious VPKI entities. Our system effectively, resiliently, and in a timely manner disseminate the authentic CRL throughout a large-scale (multi-domain) VC system.* Moreover, *we ensure that the CRL distribution incurs low overhead and prevents abuse of the distribution mechanism.*

Contributions: Our comprehensive security and privacy-preserving solution systematically addresses all key aspects of CRL-based revocation, i.e., security, privacy, and efficiency. This is based on few simple yet powerful, as it turns out, ideas. We propose making the CRL acquisition process *vehicle-centric*: each vehicle only receives the pieces of CRLs corresponding to its targeted region and its actual trip duration, i.e., obtaining only region- and time-relevant revocation information. Moreover, randomly chosen pseudonyms issued by the VPKI are selected to piggyback a notification about new CRL-update events and an authenticator for efficiently validating pieces of the latest CRL; in other words, validation of the CRL pieces *almost for free*. These novel features dramatically reduce the CRL size and CRL validation overhead, while they significantly increase its resiliency against resource depletion attacks.

In the rest of the paper, we critically survey the state-of-the-art research efforts (Sec. 2) and describe the system model (Sec. 3). We present system design (Sec. 4), followed by qualitative and quantitative analysis (Sec. 5). We then conclude the paper (Sec. 6).

2 RELATED WORK

The need to evict misbehaving or compromised [64] vehicles from a VC system is commonly accepted, because such vehicles can threaten the safety of vehicles and users and degrade transportation efficiency. CRL distribution is of central importance and it is the final and definitive line of defense [10, 26, 36, 66, 66, 71]: only the VPKI can *''ultimately''* revoke a vehicle by including its unexpired certificates' serial numbers in a CRL.

The literature proposes distribution of the CRL via RSUs [67] and car-to-car epidemic communication [38, 39, 49], with enhancements on the distribution of pieces [61, 62] evaluated in [12, 63]. A naïve solution would be to digitally sign the entire CRL and broadcast it; however, it imposes difficulties in downloading a large CRL file and exchanging it over short contact period (with an RSU or a peer). Splitting the digitally signed CRL into multiple pieces is vulnerable to *pollution* attacks: in the absence of fine-grained authentication, per CRL piece, an adversary can delay or even prevent reception by injecting fake pieces. Thus, the straightforward solution is to have the VPKI prepare the CRL, split it into multiple pieces, sign each piece, and distribute all of them across the VC system. RSUs can broadcast CRL pieces randomly or in a round-robin fashion [67], and vehicles can relay pieces until all vehicles receive all pieces necessary to reconstruct the CRL [49]. Erasure codes can be used to enhance the fault-tolerance of the CRL piece distribution in the highly volatile VC environment [13, 67].

Signing each CRL piece so that it is self-verifiable, incurs significant computation overhead, which grows linearly with the number of CRL pieces, both for the VPKI and for the receiving vehicles. Furthermore, an attacker could aggressively forge CRL pieces for a DoS attack leveraging signature verification delays [40] that can prevent vehicles from obtaining the genuine CRL pieces. A *''precode-and-hash''* scheme [60] proposes to calculate a hash value of each pre-coded piece, sign it, and disseminate it with higher priority. Each relaying node can apply a different precode to the original CRL and act as a secondary source. However, by applying different encodings to the original CRL file, another receiver cannot reconstruct the entire CRL from the pieces, encoded differently by various relaying nodes. To mitigate pollution and DoS attacks, we propose to piggyback a fingerprint (a BF [17, 57]) for CRL pieces into a subset of pseudonyms to validating CRL pieces ''for free''.

To efficiently revoke an ensemble of pseudonyms, one can enable revocation of multiple pseudonyms with a single CRL entry, to reduce the CRL size, e.g., [29, 38, 49, 76]. Despite a huge reduction in size, such schemes do not provide *perfect-forward-privacy*: upon a revocation event and CRL release, all the ''non-revoked'' but previously expired pseudonyms belonging to the evicted entity would be linked as well. Although perfect-forward-privacy can be achieved by leveraging a hash chain [39], the pseudonyms' issuer can trivially link all pseudonyms belonging to a vehicle, and thus the pseudonymously authenticated messages, towards tracking it for the entire duration of its presence in the system [29, 38, 39, 49, 76].

Compressing CRLs using a BF was proposed for compact storage of revocation entries [71], or to efficiently distribute them across the network [70, 71, 73]. However, the challenge is twofold: scalability and efficiency. The size of a CRL linearly grows with the number of revoked pseudonyms, but also a substantial portion of the ''compressed'' CRL can be irrelevant to a receiving vehicle and be left unused. Moreover, as it becomes clear in Sec. 5.1, compressing CRLs using a BF does not necessarily reduce the size of a CRL as vehicles can be provided with possibly hundreds of pseudonyms [10]. Unlike such schemes [70, 71, 73], we do not compress the CRL: our scheme disseminates only trip-relevant revocation information to vehicles and it utilizes a BF to provide a condensed authenticator for the CRL pieces. Our scheme leverages and *enhances* the functionality of the state-of-the-art VPKI system [45] towards efficiently revoking a batch of pseudonyms without compromising user privacy backwards: upon a revocation event, all pseudonyms prior to the revocation event remain unlinkable (a detailed description in Sec. 4.2).

Alternatively, vehicles could validate pseudonym status (revocation) information through OCSP [59]. However, due to intermittent VC network connectivity, significant usage of the bandwidth by time- and safety-critical operations, and substantial overhead for the VPKI (assuming the server is reachable), OCSP cannot really be used as a standalone solution [70]. A hybrid solution could rely on distributing certificate status information to other mobile nodes [30, 33--35, 53]; however, the system would be subject to the reachability (of sufficiently many cooperative) and the trustworthiness of such nodes. In our scheme, we ensure that the latest CRL is efficiently, effectively, and timely distributed among all vehicles without any assumption on persistent reachability and trustworthiness of specific mobile nodes.

Research efforts also focused on how to protect the VC systems from misbehaving nodes, by temporarily ''revoking'' (isolating) them from further access to the system [15, 58, 70, 71, 78] until connection to the VPKI is established and they are fully evicted from the system. Before the VPKI performs the ''actual'' eviction and CRL distribution, these protocols build evidence, in fact local agreement, that a given wrongdoer is present. This can serve towards isolating misbehaving vehicles before the corresponding VPKI entity takes the *''ultimate''* decision and commences the latest CRL distribution.

C2C-CC [54] and V-token [74] propose to revoke only the LTC of vehicles and let the pseudonyms expire. PUCA [31] requires the owner of the pseudonym to trigger revocation, i.e., the system cannot evict a misbehaving entity from the system. Clearly, leaving it up to the misbehaving entity, or allowing it to act for a significant period till pseudonyms expire, creates an unacceptable vulnerability window. Another line of studies proposes geo-casting a *''self-revocation''* message, by the VPKI, across a region, to wipe out the credentials from the Hardware Security Module (HSM) of a misbehaving vehicle [32, 68, 70, 71]. However, an adversary could control incoming messages, and prevent the *''self-revocation''* instruction from reaching the HSM, i.e., such schemes alone cannot guarantee the trustworthiness of the system against misbehavior unless the VPKI distributes the CRL enabling legitimate vehicles to defend themselves against misbehavior or faulty peers.

Alternatively, the VPKI could provide vehicles for a long period, e.g., 25 years, worth of pseudonyms with a decryption key for, e.g., a weekly batch of pseudonyms, delivered periodically [48]. This would eliminate the need for bidirectional connectivity to the VPKI to obtain pseudonyms. To evict a vehicle, the VPKI can stop delivering the corresponding decryption key to the vehicle HSM. Still, it is imperative to distribute the CRL and cover the (weekly) period and the corresponding revoked pseudonyms. Furthermore, having released a CRL towards the end of a week, signed messages with the private keys corresponding to the recently revoked pseudonyms (included in the CRL) can be linked, i.e., backwards-trackable for a week (no *perfect-forward-privacy* for that period) [1].

Outside the VC realm, a recent comparative evaluation of classic Internet schemes is available [20]. Such schemes, e.g., [19, 22, 42, 50, 55, 56, 75], cannot be leveraged due to the nature of VC systems, i.e., short-lived pseudonyms, highly dynamic intermittent connectivity, and resource constraints. For example, CRLite [50] stores CRLs in a *filter-cascade* BF without any false positive or false negative; however, this necessitates little change in the set of revoked and non-revoked certificates. Obviously, this contradicts *on-demand* pseudonym acquisition strategies for VC systems, e.g., [16, 29, 31, 43--46, 52, 74], which are more efficient (than preloading for a long duration, e.g., [48]) in terms of pseudonym utilization and revocation, thus more effective in fending off misbehavior.

3 MODEL AND REQUIREMENTS

3.1 System Model and Assumptions

A VPKI consists of a set of Certification Authorities (CAs) with distinct roles: the Root CA (RCA), the highest-level authority, certifies other lower-level authorities; the Long Term CA (LTCA) is responsible for the vehicle registration and the Long Term Certificate (LTC) issuance, and the Pseudonym CA (PCA) issues pseudonyms for the registered vehicles. Pseudonyms have a lifetime (a validity period), typically ranging from minutes to hours; in principle, the shorter the pseudonym lifetime is, the higher the unlinkability and thus the higher privacy protection can be achieved. We assume that each vehicle is registered only with its *Home-LTCA (H-LTCA)*, the *policy decision and enforcement point*, reachable by the registered vehicles. Without loss of generality, a *domain* can be defined as a set of vehicles in a region, registered with the H-LTCA, subject to the same administrative regulations and policies [47]. There can be several PCAs, each active in one or more domains. Each vehicle can cross in to *foreign* domains and communicate with the *Foreign-LTCA (F-LTCA)* towards obtaining pseudonyms, i.e., a new set of pseudonyms when entering a new domain, to operate as a native vehicle in that region. Trust between two domains can be established with the help of the RCA, or through cross certification. Moreover, the certificates of higher-level authorities are installed in the On-Board Units (OBUs), which are loosely synchronized with the VPKI servers. The RSUs could be deployed by other authorities than the VPKI ones, thus they only expose minimal information, e.g., IP address and location, to the corresponding PCAs.

All vehicles (OBUs) registered in the system are provided with HSMs, ensuring that private keys never leave the HSM. Moreover, we assume that there is a misbehavior detection system, e.g., [15], that triggers the revocation[1]. The Resolution Authority (RA) can initiate a process to resolve and revoke all pseudonyms of a misbehaving vehicle: it interacts with the corresponding PCAs and LTCA (a detailed protocol description, e.g., in [44, 45]) to resolve and revoke all credentials issued for a misbehaving vehicle. Consequently, the misbehaving vehicle can no longer obtain credentials from the VPKI. The VPKI is responsible for distributing the CRLs and notifying all legitimate entities about the revocation; this implies a new CRL-update event.[2]

[1]The faulty behavior detection depends on, e.g., data-centric plausibility and consistency checks, and it is orthogonal to this investigation.
[2]The revocation information of other system entities, e.g., VPKI entities, need to be distributed as well. Here, we only focus on the distribution of revoked pseudonyms.

3.2 Adversarial Model

We extend the general adversary model in secure vehicular communications [65] to include VPKI entities that are *honest-but-curious*, i.e., entities complying with security protocols and policies, but motivated to profile users. In a multi-domain VC environment, internal adversaries, i.e., malicious, compromised, or non-cooperative clients, and external adversaries, i.e., unauthorized entities, raise four challenges. More specifically in the context of this work, adversaries can try to (i) exclude revoked pseudonym serial numbers from a CRL, (ii) add valid pseudonyms by forging a fake CRL (piece), or (iii) prevent legitimate entities from obtaining genuine and the most up-to-date CRL (pieces), or delay the CRL distribution by replaying old, spreading fake CRL (pieces), or performing a DoS attack. This allows wrong-doers to remain operational in the VC system using their current revoked pseudonym sets. Moreover, they might be simply non-cooperative or malicious, tempted to prevent other vehicles from receiving a notification on a new CRL-update event, thus preventing them from requesting to download the CRLs. Lastly, (iv) VPKI entities (in collusion with vehicle communication observers) could potentially link messages signed under (non-revoked but expired) pseudonyms prior to the revocation events, e.g., inferring sensitive information from the CRLs towards linking pseudonyms, and thus tracking vehicles backwards. The PCAs operating in a domain (or across domains) could also collude, i.e., share information that each of them individually has, to harm user privacy.[3]

3.3 Requirements

Security and privacy requirements for V2X communications have been specified in the literature, e.g., as early as [65], and additional requirements specifically for VPKI entities in [45]. Next, we compile security and privacy, as well as functional and performance, requirements for the CRL distribution problem.

R1. Fine-grained authentication, integrity, and non-repudiation: Each CRL (piece) should be authenticated and its integrity be protected, i.e., preventing alternation or replays. Moreover, each CRL (piece) should be non-repudiably connected to its originator (the VPKI entity).

R2. Unlinkability (perfect-forward-privacy): CRLs should not enable any observer (even in collusion with a single VPKI entity) to link pseudonyms (and thus the corresponding signed messages) prior to their revocation. In fact, upon a revocation event, all non-revoked previously expired pseudonyms of an evicted vehicle should remain unlinkable.

R3. Availability: The system should ensure any legitimate vehicle can obtain the latest CRL within a reasonable time interval despite of benign failures, e.g., system faults or crashes, or network outages, e.g., intermittent connectivity. Moreover, the system should be resilient to active disruptions, including resource depletion attacks.

R4. Efficiency: Generating, validating, and disseminating the CRL (pieces) and revocation event notification should be efficient and scalable even if the number of vehicles and credentials grow, i.e., incurring low computation and communication overhead. Moreover, a small fraction of bandwidth should be used for CRL distribution, in order not to interfere with transportation safety- and time-critical operations. However, allocation of a small amount of bandwidth in a timely fashion should be sufficient to distribute CRLs to all legitimate vehicles.

R5. Explicit and/or implicit notification on revocation events: The system should notify, explicitly or implicitly, every legitimate vehicle within the system (domain) regarding revocation events and then CRL-updates (availability of new revocation information).

4 DESIGN

4.1 Motivation and Overview

Preliminary assumptions: We leverage the state-of-the-art VPKI system [45] that provides pseudonyms in an *on-demand* fashion: each vehicle *"decides"* when to trigger the pseudonym acquisition process based on various factors [43]. Such a scheme requires sparse connectivity to the VPKI, but it facilitates an OBU to be *preloaded* with pseudonyms proactively, covering a longer period, e.g., a week or a month, should the connectivity be expected heavily intermittent. The efficiency, scalability and robustness of the VPKI system is systematically investigated [43, 45] with the VPKI handles a large workload. Moreover, it enhances user privacy, notably preventing linking pseudonyms based on *timing information* (the instance of issuance and the pseudonym lifetime) as well as offers strong user privacy protection even in the presence of *honest-but-curious* VPKI entities. More precisely, a universally fixed interval, Γ, is specified by the H-LTCA and all pseudonyms in that domain are issued with the lifetime (τ_P) aligned with the VPKI clock. Vehicles obtain pseudonyms on-the-fly as they operate, and the number of pseudonyms in a request is $\frac{\Gamma}{\tau_p}$, i.e., no prior calculation needed. As a result of this policy, at any point in time, all the vehicles transmit using pseudonyms that are indistinguishable thanks to this time alignment, i.e., eliminating any distinction among pseudonym sets of different vehicles, thus enhancing user privacy. We leverage and *enhance* the functionality of this VPKI system; in particular, our solution necessitates two modifications during pseudonym acquisition process, notably (i) implicitly binding pseudonyms issued to a given requester per Γ, and (ii) integrating a fingerprint into a subset of the pseudonyms for efficient CRL validation.

High-level overview: The default policy is to distribute all revocation information to all vehicles. Nonetheless, this approach ignores the locality, the temporal nature of pseudonyms, and other constraints, e.g., the average daily commute time. Locality could be geographical, i.e., credentials relative to the corresponding region, and temporal, i.e., relevance to the lifetime of pseudonyms with respect to the trip duration of a vehicle. To efficiently, effectively, and timely distribute the CRLs across the V2X network, we propose making the CRL acquisition process *vehicle-centric*, i.e., through *a content-based and context-sensitive "publish-subscribe"* scheme [27, 41].

Fig. 1 shows that by starting a new trip, each vehicle only subscribes to receive the pieces of CRLs, i.e., the content, corresponding to its actual trip duration and its targeted region, i.e., the context. To reap the benefits of the ephemeral nature pseudonyms and the timely-aligned pseudonym provisioning policy, towards an effective, efficient, and scalable CRL distribution, a fixed interval,

[3]Note that *"malicious"* VPKI entities could attempt to influence the distribution of CRLs, e.g., manipulating the CRL entries unlawfully; this is out of the scope of our honest-but-curious adversarial model.

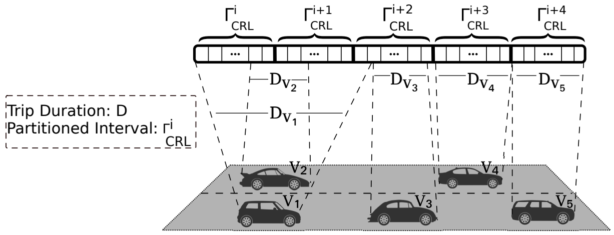


Figure 1: CRL as a Stream: V_1 **subscribes to** $\{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}, \Gamma^{i+2}_{CRL}\}$; $V_2 : \{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}\}$; $V_3 : \{\Gamma^{i+2}_{CRL}\}$; $V_4 : \{\Gamma^{i+3}_{CRL}\}$; **and** $V_5 : \{\Gamma^{i+4}_{CRL}\}$.

Γ_{CRL}, is predetermined by the PCAs in the domain. They publicize revoked pseudonyms whose lifetimes fall within Γ_{CRL}, i.e., distributing only the serial number of these pseudonyms rather than publishing the entire CRL. Note that Γ, the universally fixed interval to obtain pseudonyms [45], and Γ_{CRL} are not necessarily aligned due to the unpredictable nature of revocation events.

When a vehicle reliably connects to the VPKI, it can obtain the *"necessary"* CRL pieces corresponding to its trip duration during the pseudonym acquisition phase. However, if reliable connectivity is not guaranteed, or if a vehicle obtained (possibly preloaded with enough) pseudonyms in advance, or a new revocation event happens, one can be notified about a new CRL-update (revocation) event: a signed fingerprint (a Bloom Filter (BF) [17, 57]) of CRL pieces is broadcasted by RSUs and it is integrated in a subset of recently issued pseudonyms, this way readily broadcasted by vehicles (termed *fingerprint-carrier* nodes) along with their Cooperative Awareness Messages (CAMs). This essentially piggybacks a notification about the latest CRL-update event and an authenticator for validating CRL pieces. This provides CRL validation for free: pseudonyms are readily validated by the receiving vehicles since each vehicle verifies the signature on a pseudonym before validating the content of a CAM, i.e., the verification of CRL pieces does not incur extra computation overhead. This eliminates the need for signature verification, but a BF membership test, for each CRL piece as the fingerprint is signed with the private key of the PCA.

Our scheme does not require prior knowledge on trip duration in order to obtain CRLs, i.e., a vehicle can be oblivious to the trip duration. In fact, such information would not be relevant to the CRL dissemination: due to the unpredictable nature of revocation events, the PCAs disseminate at each point revoked pseudonyms whose lifetimes fall within a Γ_{CRL} interval. As long as a vehicle moves inside a domain, it does not need to receive CRLs from other domains: all vehicles in the domain are issued pseudonyms by the PCAs in that domain. In other words, our scheme does not require any communication and cooperation between RSUs and PCAs from different domains on CRL construction and distribution tasks; only PCAs-RSUs collaboration within a domain. The PCAs operating in a domain construct the CRLs and push the CRL pieces to the RSUs so that the RSUs broadcast the CRL pieces for the current Γ_{CRL}.

Fig. 2 illustrates an example of 24 revoked pseudonyms to be distributed. A vehicle traveling within Γ^{1}_{CRL} would possibly only face revoked pseudonyms with a lifetime falling in that interval, 6 pseudonyms, shown in black, instead of all 24 entries (the blurred pseudonyms are expired, thus not included in the CRL). These 6 revoked pseudonyms within Γ^{1}_{CRL} can be implicitly bound without compromising their unlinkability prior to the revocation event, in

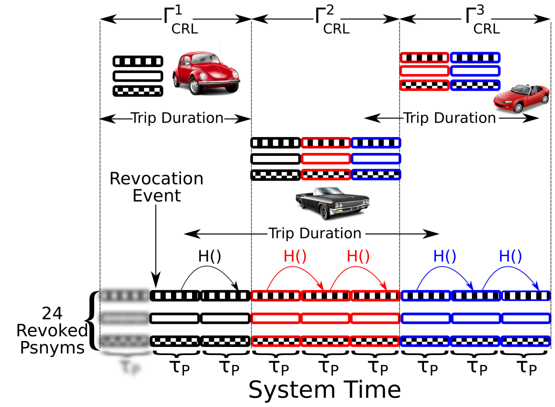


Figure 2: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration.

a way that one can simply derive subsequent pseudonyms from an anchor (the blurred pseudonyms are non-revoked but expired and they cannot be linked to the revoked ones; this becomes clear later). Thus, in this example, distributing 3 entries for that vehicle is sufficient. Another vehicle, however, traveling for a longer duration, e.g., from the middle of Γ^{1}_{CRL} till the beginning of Γ^{3}_{CRL}, would need to be provided with all 24 revocation entries, i.e., requiring 9 entries to derive all 24 revoked pseudonyms.

In a more realistic example, assume there are 1 million vehicles in the system, each has 6 hours worth of pseudonyms (72 pseudonyms per day with $\Gamma = 30$ min and $\tau_P = 5$ min, i.e., 6 pseudonyms per Γ), all are issued timely aligned with the rest with non-overlapping intervals [45]. Suppose 1 percent of them are compromised or their sensors became faulty and thus evicted from the system. As a result, the revocation information to be disseminated for a day contains 720,000 entires, thus a CRL of around 22 MB (with 256-bit long serial numbers per pseudonym). By implicitly binding pseudonyms belonging to each OBU, one can distribute 1 entry for a batch of revoked pseudonyms per Γ (with some additional information), in total, 12 entries per revoked vehicle instead of 72 entries. Thus, the size of the CRL for that day becomes 7.3 MB, with 120,000 entries (with 256-bit serial numbers and 256-bit of complementary information for each entry). This already shows a significant reduction of the CRL size. However, distributing all that revocation information ignores the temporal nature of pseudonyms and the vehicle trip duration; it is more effective to distribute revocation information for a protocol-selectable period in the near future. Therefore, when a vehicle is to travel approximately within a Γ_{CRL} interval, assumed for example to be 30 min, it will only receive pieces of information for that Γ_{CRL}, i.e., around 10,000 entries and thus a CRL size of 625 KB instead of 22 MB, i.e., 3 orders of magnitude reduction of the CRL size distributed at any point in time.

4.2 Security Protocols

In a nutshell, the PCAs operating in a domain construct the CRLs by sorting the revoked pseudonyms based on their validity periods in a Γ_{CRL} interval and push them to the RSUs (Sec. 4.2.2). For ease of exposition, we assume there is one PCA, even though the extension of our scheme with multiple PCAs within a given domain is straightforward. RSUs and fingerprint-carrier peers publish the

Table 1: Notation Used in the Protocols.

Notation	Description	Notation	Description
$(P_v^i)_{pca}, P_v^i$	a valid psnym signed by the PCA	$Append()$	appending a revoked psnym SN to CRLs
(K_v^i, k_v^i)	psnym pub./priv. key pairs	BFTest()	BF membership test
$(K_{pca}; Lk_{pca})$	long-term pub./priv. key pairs	p, K	false positive rate, optimal hash functions
$(msg)_{\sigma_v}$	signed msg with vehicle's priv. key	Γ	interval to issue time-aligned psnyms
LTC	Long Term Certificate	Γ_{CRL}	interval to release CRLs
t_{now}, t_s, t_e	a fresh, starting, ending timestamp	RIK	revocation identifiable key
$T_{timeout}$	response reception timeout	$\mathbb{B}$	max. bandwidth for CRL distribution
$n\text{-}tkt$, $(n\text{-}tkt)_{ltca}$	a native ticket	$\mathbb{R}$	revocation rate
Id_{req}, Id_{res}	request/response identifiers	N	total number of CRL pieces in each Γ_{CRL}
SN	psnym serial number	n	number of remaining psnyms in each batch
$Sign(Lk_{ca}, msg)$	signing a msg with CA's priv. key	k	index of the first revoked psnym
$Verify(LTC_{ca}, msg)$	verifying with the CA's pub. key	CRL_v	CRL version
$GenRnd(), rand(0,*)$	GEN. a random number, or in range	$\emptyset$	Null or empty vector
$H^k(), H$	hash function (k times), hash value	k, j, m, ζ	temporary variables

Protocol 1 Issuing Pseudonyms (by the PCA)

1: **procedure** IssuePsnyms(Req)
2: $Req \rightarrow (Id_{req}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, \cdots, (K_v^n)_{\sigma_{k_v^n}}\}, nonce, t_{now})$
3: Verify(LTC_{ltca}, $(tkt)_{\sigma_{ltca}}$)
4: $Rnd_v \leftarrow GenRnd()$
5: **for** i:=1 to **n do**
6: **Begin**
7: Verify(K_v^i, $(K_v^i)_{\sigma_{k_v^i}}$)
8: $RIK_{P_v^i} \leftarrow H(IK_{tkt}||K_v^i||t_s^i||t_e^i||H^i(Rnd_v))$
9: **if** $i = 1$ **then**
10: $SN^i \leftarrow H(RIK_{P_v^i}||H^i(Rnd_v))$
11: **else**
12: $SN^i \leftarrow H(SN^{i-1}||H^i(Rnd_v))$
13: **end if**
14: $\zeta \leftarrow (SN^i, K_v^i, CRL_v, BF_{\Gamma_{CRL}^i}, RIK_{P_v^i}, t_s^i, t_e^i)$
15: $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
16: **End**
17: **return** $(Id_{res}, \{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, Rnd_v, nonce{+}1, t_{now})$
18: **end procedure**

CRL-update notification and the CRL pieces (Sec. 4.2.3). Upon receiving a new revocation event, each vehicle broadcasts a query to its neighbors to fetch the (missing) pieces of the CRL, e.g., similarly to [23], corresponding to its actual trip duration (Sec. 4.2.4). Finally, it parses recovered CRL pieces and stores them locally (Sec. 4.2.5).

Beyond CRL distribution protocols, we provide a modified pseudonym acquisition process (Sec. 4.2.1): all pseudonyms belonging to a requester in a Γ are issued in a way that does not link them, unless the PCA reveals only the first revoked pseudonym serial number in a Γ interval. Moreover, a fraction of pseudonyms is equipped with a fingerprint of CRL pieces in a Γ interval, to facilitate fast validation of CRL pieces. The notation is given in Table 1.

4.2.1 *Pseudonym Acquisition Process (Protocol 1).*

A vehicle first requests an anonymous ticket [43, 44] from its H-LTCA, using it to interact with the desired PCA to obtain pseudonyms. Upon reception of a valid ticket, it generates Elliptic Curve Digital Signature Algorithm (ECDSA) public/private key pairs [10, 26] and sends the request to the PCA [43, 44]. Vehicle-LTCA is over mutually authenticated Transport Layer Security (TLS) [24] tunnels (or Datagram TLS (DTLS) [72]) and the vehicle-PCA communication is over a unidirectional (server-only) authenticated TLS (or DTLS).

Having received a request, the PCA verifies the ticket signed by the H-LTCA (assuming trust is established between the two) (steps 1.2–1.3). Then, the PCA generates a random number (step 1.4) and initiates a proof-of-possession protocol to verify the ownership of the corresponding private keys by the vehicle (step 1.7). Then, it

Protocol 2 CRL Construction (by the PCA)

1: **procedure** GenCRL(Γ_{CRL}^i, $\mathbb{B}$)
2: $Piece_{\Gamma_{CRL}^i} \leftarrow \emptyset$
3: **repeat**
4: $\{SN_P^k, H_{Rnd_v}^k, n\} \leftarrow fetchRevokedPsnyms(\Gamma_{CRL}^i)$
5: **if** $SN_P^k \neq Null$ **then**
6: $Piece_{\Gamma_{CRL}^i} \leftarrow Append(\{SN_P^k, H_{Rnd_v}^k, n\})$
7: **end if**
8: **until** $SN_P^k == Null$
9: $N \leftarrow \left\lceil \dfrac{size(Piece_{\Gamma_{CRL}^i})}{\mathbb{B}} \right\rceil$ ▷ calculating number of pieces with a given $\mathbb{B}$
10: **for** $j \leftarrow 0$, N **do** ▷ N: number of pieces in Γ_{CRL}^i
11: $Piece_{\Gamma_{CRL}^i}^j \leftarrow Split(Piece_{\Gamma_{CRL}^i}, \mathbb{B}, N)$ ▷ splitting into N pieces
12: **end for**
13: **return** $\{(Piece_{\Gamma_{CRL}^i}^1), \ldots, (Piece_{\Gamma_{CRL}^i}^N)\}$
14: **end procedure**

calculates $H(IK_{tkt}||K_v^i||t_s^i||t_e^i||H^i(Rnd_v))^4$, the *"revocation identifiable key"* (*RIK*). This essentially prevents a compromised PCA from mapping a different ticket during resolution process (step 1.8). The PCA implicitly correlates a batch of pseudonyms belonging to each requester (steps 1.9–1.13). This essentially enables efficient distribution of the CRL: the PCA only needs to include one entry per batch of pseudonyms without compromising their unlinkability. Finally, the PCA issues the pseudonyms (steps 1.14–1.15) and delivers the response (step 1.17). Note that a PCA randomly selects some of the pseudonyms to be fingerprint-carriers by integrating a BF of all CRL pieces within a Γ_{CRL} ($BF_{\Gamma_{CRL}^i}$) (step 1.14). This parameter (fraction of fingerprint-carriers) can be set based on different factors, e.g., frequency of revocation events and coverage of deployed RSUs, which are beyond the scope of this work.

4.2.2 *PCA Operation for CRL Construction (Protocol 2).*

When a vehicle is to be evicted, the PCA sorts revoked pseudonyms based on the pseudonyms validity intervals in each Γ_{CRL}. It then appends the following data for each batch of pseudonyms: (i) the serial number of the first revoked pseudonym in the chain (SN^i), (ii) a hash value ($H_{Rnd_v}^i$), and (iii) the number of remaining pseudonyms in this batch (n) (steps 2.2– 2.8). It then splits the CRL into multiple pieces according to the maximum allocated bandwidth, i.e., system parameter $\mathbb{B}$, for CRL distribution (steps 2.9– 2.13). The number of revocation entries is proportional to the number of pseudonyms and vehicles, and revocation events, e.g., due to vehicle-compromising malware propagation, evaluated in Sec. 5.

4.2.3 *Operations for Publishing the CRL (Protocol 3).*

Each RSU continuously broadcasts the signed fingerprint of CRL pieces, to notify vehicles in a region about any new revocation event. The transmission rate of the signed fingerprint corresponding to the current Γ_{CRL}^i can gradually decrease towards the end of Γ_{CRL}^i; instead, the transmission rate of the signed fingerprint for Γ_{CRL}^{i+1} can moderately increase. This "ensures" that all legitimate vehicles are notified about a new revocation event, thus being capable to request and efficiently validate CRL pieces (evaluated in Fig. 6.b).

[4] IK_{tkt} in a ticket prevents even a compromised H-LTCA from mapping the ticket to a different LTC during resolution process [45].

Protocol 3 Publishing CRLs (by the OBUs)

1: **procedure** PublishCRL()
2: $\{(Id_{req}, \Gamma^i_{CRL}, [indexes])\} = receiveQuery((\zeta)_{\sigma_{P^i_v}})$
3: $Verify(P^i_v, (\zeta)_{\sigma_{P^i_v}})$
4: $CRL^*_{\Gamma^i_{CRL}} = search_{local}(\Gamma^i_{CRL})$ ▷ search local repository
5: $j \leftarrow rand(0, *)$ ▷ randomly select one of the available pieces
6: **if** $CRL^j_{\Gamma^i_{CRL}} \neq \emptyset$ **then**
7: $broadcast(\{Id_{res}, CRL^j_{\Gamma^i_{CRL}}\})$
8: **end if**
9: **end procedure**

Protocol 4 Subscribing to CRL Pieces (by the OBUs)

1: **procedure** SubscribeCRL(Γ^i_{CRL}, N)
2: $resp_{final} \leftarrow \emptyset, j \leftarrow 0, t \leftarrow t_{now} + T_{timeout}$
3: **repeat**
4: $\zeta \leftarrow (Id_{req}, \Gamma^i_{CRL}, [missing\ pieces\ indexes])$
5: $(\zeta)_{\sigma_v} \leftarrow Sign(k^i_v, \zeta)$
6: $broadcast((\zeta)_{\sigma_{P^i_v}}, P^i_v)$
7: $Piece^j_{\Gamma^i_{CRL}} \leftarrow receiveBefore(t)$
8: **if** $BFTest(Piece^j_{\Gamma^i_{CRL}}, BF_{\Gamma^i_{CRL}})$ **then**
9: $resp_{final} \leftarrow Store(Piece^j_{\Gamma^i_{CRL}})$ ▷ storing in local repository
10: **end if**
11: $j \leftarrow j + 1$
12: **until** $j > N$
13: **return** $resp_{final}$
14: **end procedure**

Upon reception and validation of a query, an RSU commences transmission across the wireless data link with a low-rate transmission (without any acknowledgment from peers).

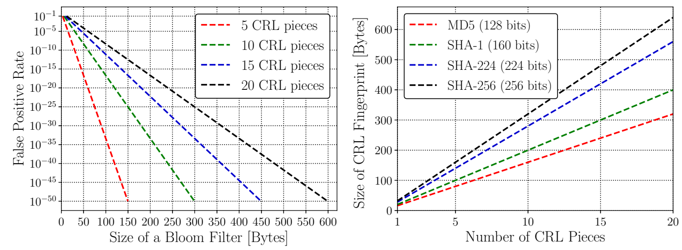
Upon receiving an authentic query for the missing CRL pieces (steps 3.2–3.3) by a neighboring vehicle, a vehicle searches its local repository and randomly chooses one of the requested pieces and broadcasts it (steps 3.4–3.8). The maximum allocated bandwidth for CRL distribution is $\mathbb{B}$, chosen to be much smaller than C, the bandwidth the data link support ($\mathbb{B} \ll C$). Such a rate limiting mechanism ensures that a compromised insider cannot abuse the allocated bandwidth towards performing a DoS attack, thus CRL distribution does not interfere with other safety-critical operations.

4.2.4 *Operations for CRL Subscription (Protocol 4).*

Each vehicle can receive necessary CRL pieces corresponding to its actual trip duration from nearby RSUs or neighboring vehicles. A vehicle broadcasts a signed query to its neighbors, to receive the missing pieces of the revocation information of Γ^i_{CRL} during which the vehicle wishes to travel (steps 4.2– 4.6). Having received a CRL piece, it simply validates the piece by testing against the signed fingerprint (already obtained from RSUs in vicinity or integrated in a subset of recently issued pseudonyms broadcasted in the network). If the BF test is successful, it accepts that piece and keeps requesting until successfully receiving all remaining pieces (steps 4.7– 4.12).

4.2.5 *Operations for Parsing CRL.*

Upon reception and validation of a CRL piece, each vehicle derives the revoked pseudonym serial numbers from the obtained hash anchors, by calculating a hash value n times: $H(SN^i||H(H^i_{Rnd_v}))$. Revocation entries can be stored in local storage, e.g., [33], and searched with $O(log(n))$ time complexity. To enhance revocation status validation, a vehicle could generate a BF locally [39] with constant computational cost ($O(1)$) for insertions and search operations but at a cost of a false positive rate. Note that the revocation entries are stored for the period they are valid for, i.e., within a Γ^i_{CRL} interval.



(a) Vehicle-centric scheme **(b) Precode-and-hash scheme [60]**

Figure 3: Extra overhead for CRL fingerprints.

5 SCHEME ANALYSIS AND EVALUATION

We first discuss how our scheme satisfies the security and privacy requirements, as well as operational requirements defined in Sec. 3.3 and then demonstrate quantitatively its efficiency, scalability, and resiliency through an extensive experimental evaluation.

5.1 Qualitative Analysis

Fine-grained authentication, integrity, and non-repudiation: The authenticity and integrity of each CRL piece is validated by testing each piece against the fingerprint, periodically broadcasted by RSUs and integrated in a subset of recently issued pseudonyms (R1). Moreover, no PCA can deny the inclusion of pseudonym serial number as the fingerprint of CRL pieces is signed with the PCA's private key (R1). Furthermore, each query to obtain CRL pieces is authenticated, in fact signed with the current valid pseudonym of the vehicle, thus preventing from abusing mechanism. If a *legitimate-looking* node aggressively requests CRL pieces, responding to such requests can be of the lowest priority and they are reported as potential misbehavior.

Representing CRL pieces in a space-efficient BF trades off communication overhead for a false positive rate (p). Fig. 3.a shows that the BF size linearly increases as the false positive rate decreases. For example, for 10 CRL pieces covering one Γ_{CRL}, and $p = 10^{-20}$ (with the optimal number of hash functions), the BF size and thus the overhead for each pseudonym is 120 bytes. This eliminates the need to sign each CRL piece. However, one might target the false positive rate of a BF towards generating a fake piece of CRL to be accepted as legitimate. This is different from a pollution or a Distributed DoS (DDoS) attack: not only would it prevent a legitimate vehicle from obtaining a genuine CRL piece, but also disseminate an *authentic-looking* piece that passes the BF test; in fact, such attacks can rely on sheer computational power.

Our scheme resists such attacks that attempt to exclude revoked pseudonym serial numbers or add valid ones by forging a fake

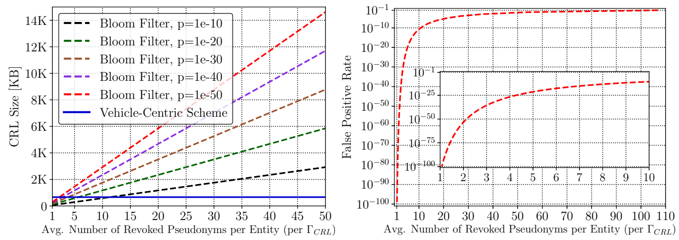
CRL piece that passes the BF test.[5] An adversary could buy top-notch bitcoin-mining hardware, Antminer-S9 [6] (14TH/s, \$3,000). If $\Gamma_{CRL} = 1$ hour and $p = 10^{-20}$, and the optimal number of hash functions, $K = 67$, the adversary needs 132,936 Antminer-S9 (\$400M) to generate a bogus piece within Γ_{CRL} ($\frac{10^{20} \times 67}{14 \times 10^{12}}$). Alternatively, he could join AntPool [5], one of the largest Bitcoin mining pools, ($1,604,608\ TH/s$) to generate a fake piece in 70 min, which might seem to be practical. However, if $p = 10^{-22}$ (with $K = 73$) or even $p = 10^{-23}$ (with $K = 76$), the adversary would need 5 or 55 days, respectively ($\frac{10^{22} \times 73}{1.6 \times 10^{18}} = 126h$, $\frac{10^{23} \times 76}{1.6 \times 10^{18}} = 1,319h$). With inherently short τ_P (important for unlinkability and thus privacy) and Γ_{CRL}, proper choice of p makes attacks infeasible; in other words, irrelevant, as forged pieces refer to already expired credentials. Upon receiving conflicting pieces, vehicles report misbehavior to the VPKI to take appropriate actions, e.g., adjusting p. The results of our experiments in Sec. 5.2 rely on $p = 10^{-30}$ and $K = 100$.

The PCA can concatenate the hash values for each CRL piece [60], or alternatively truncate the output of hash functions. Fig. 3.b shows the size of a CRL fingerprint with different hash functions. For instance, by employing *precode-and-hash* with SHA1 (20 bytes output size) [60], the size of a fingerprint for 20 CRL pieces becomes 400 bytes; whereas employing our scheme results in an extra overhead of 311 bytes ($p = 10^{-25}$) or 371 bytes for the extremely low false positive rate ($p = 10^{-30}$).

Unlinkability (perfect-forward-privacy): Upon a revocation event and CRL release, an external observer can try to link the revoked pseudonyms backwards (towards the beginning of the Γ interval). However, it is infeasible to link the previously non-revoked (but expired) pseudonyms belonging to a misbehaving vehicle due to the utilization of a hash-chain during pseudonym issuance process ($SN^i \leftarrow H(RIK_{P^i_v} || H^i_{Rnd_v})$ or $SN^i \leftarrow H(SN^{i-1} || H(H^i_{Rnd_v}))$, i.e., strong user privacy protection for a period, during which the vehicle was not compromised (R2).

In collusion with V2X observers, honest-but-curious PCAs operating in a given domain might be tempted to infer sensitive information from the pseudonyms, e.g., timing information, or, in our context, the CRLs, towards linking pseudonym sets and tracking a vehicle. However, all the issued pseudonyms are aligned with global system time (PCA clock), thus, there is no distinction among pseudonyms based on pseudonym timing information. Moreover, the CRLs do not disclose extra information to harm user privacy[6]. Moreover, PCAs randomly select a subset of pseudonyms to be fingerprint-carries; thus, correlating any of these pseudonyms does not imply that they belong to the same vehicle (R2).

Availability: We leverage RSUs and car-to-car epidemic distribution to disseminate CRL pieces and signed fingerprints for increased availability or intermittent connectivity (R3). The resilience to pollution and DDoS attacks stems from three factors: (i) a huge reduction of the CRL size, notably because of distributing CRL information only for relevant periods of time, (ii) very efficient verification of CRL pieces, i.e., testing against a BF with hash and not signature validation, and (iii) integrating the fingerprint of CRL pieces in a subset of pseudonyms (R3).



(a) CRL size comparison

(b) C^{2}RL as a factor of false positive rate

Figure 4: (a) CRL size comparison for C^{2}RL and vehicle-centric scheme (10,000 revoked vehicles). (b) Achieving vehicle-centric comparable CRL size for the C^{2}RL scheme.

Efficiency: The efficiency stems from the efficient construction of an authenticator for CRL pieces (minimal overhead on the PCA side), fast verification of each piece (minimal overhead on the vehicle side), and implicit binding of a batch of pseudonyms. Moreover, leveraging recurrent interactions with the VPKI, which issues time-aligned pseudonyms for all vehicles, and distributing CRLs with respect to locality, the ephemeral nature of credentials, and the average trip duration enhances efficiency (R4). We allocate a small fraction of bandwidth for CRL distribution and we apply a rate limiting mechanism to prevent abuse of the mechanism (R3-R4). However, allocating a small amount of bandwidth is sufficient to timely distribute CRLs to practically all legitimate vehicles within the system (R4), as demonstrated in Sec. 5.2.1. Note that if pseudonyms were provided for a long period and vehicles had only unidirectional connectivity [48], then the VPKI cannot integrate new information into the pseudonyms for efficiency reasons. Thus, the signed fingerprint of CRL pieces would need to be disseminated through RSUs on a weekly basis.

Explicit and/or implicit notification on revocation events: Malicious entities might try to prevent other legitimate vehicles from receiving CRL-update notifications, thus preventing them from requesting the latest CRL, i.e., compromising availability and essentially harming the VC system security (as evicted nodes would remain undetected). RSUs periodically broadcast the signed fingerprint, corresponding to all CRL pieces of a given Γ_{CRL}, to ensure reception of the CRL validation authenticator in a region. Moreover, the PCAs randomly choose a subset of recently issued pseudonyms to piggyback the CRL-update notification. Vehicles beacon CAMs at a high rate, each signed with the private key of a pseudonym that possibly carries a notification about a CRL-update event and attach the pseudonym to a significant fraction of CAMs, in fact free notification about a revocation event at any point in time in the system (R5). Further evidence to the availability, the resiliency, and the efficiency, is provided through the detailed experimental evaluation in Sec. 5.2.

CRL size comparison: The size of a CRL by compressing the revocation information into a BF, i.e., C^{2}RL scheme [70, 71, 73], is $m_{BF} = -\frac{N \times M \times ln\, p}{(ln 2)^2}$ [77], where N is the total number of compromised vehicles, M is the average number of revoked pseudonyms

[5]Generating a fake BF with completely different valid pseudonyms serial number necessitates accessing at least, e.g., 10^{20}, valid pseudonyms, i.e., a more powerful adversary (*malicious VPKI entities*), and is beyond the scope of our adversarial model.
[6]Each PCA can trivially link the issued pseudonyms for the same vehicle as a response to a single request. However, one can configure the system to achieve *full unlinkability*, i.e., Γ is set equal to τ_P and force obtaining each single pseudonym with a different ticket. This implies that even honest-but-curious PCAs cannot link any two pseudonyms issued for a single vehicle, but it would be impractical in most setting.

Table 2: Simulation Parameters (LuST dataset).

Parameters	Value	Parameters	Value
CRL/Fingerprint TX interval	0.5s/5s	Pseudonym lifetime	30s-600s
Carrier frequency	5.89 GHz	Area size	50 KM × 50 KM
TX power	20mW	Number of vehicles	138,259
Physical layer bit-rate	18Mbps	Number of trips	287,939
Sensitivity	-89dBm	Average trip duration	692.81s
Thermal noise	-110dBm	Duration of simulation	4 hour (7-9, 17-19)
CRL dist. Bandwidth ($\mathbb{B}$)	10, 25, 50 KB/s	Γ	1-60 min
Number of RSUs	100	Γ_{CRL}	60 min

Table 3: LuST Revocation Information ($\mathbb{R}$ = 1%, $\mathbb{B}$ = $10KB/s$).

Pseudonym Lifetime	Number of Psnyms	Number of Revoked Psnyms	Average Number per Γ_{CRL}	Number of Pieces
τ_P=30s	3,425,565	34,256	1,428	12
τ_P=60s	1,712,782	17,128	710	6
τ_P=300s	342,556	3,426	143	2
τ_P=600s	171,278	1,713	72	1

Table 4: Simulation Parameters for LuST Dataset (τ_P = $60s$).

Revocation Rate ($\mathbb{R}$)	Baseline Scheme				Vehicle-Centric Scheme			
	CRL Entries	10 KB/s Pieces	25 KB/s Pieces	50 KB/s Pieces	CRL Entries	10 KB/s Pieces	25 KB/s Pieces	50 KB/s Pieces
0.5%	8,500	70	30	15	355	3	2	1
1%	17,000	140	59	30	710	6	3	2
2%	34,000	279	117	59	1,417	12	5	3
3%	51,000	419	175	89	2,125	18	8	4
4%	68,000	558	233	118	2,834	24	10	5
5%	85,000	697	291	148	3,542	30	13	7

per vehicle per Γ_{CRL}, and p is the probability of false positive[7]. Fig. 4.a illustrates that the size of a CRL with C^{2}RL grows linearly with M. Using our vehicle-centric scheme, it is sufficient to disclose one entry to revoke all pseudonyms of an evicted vehicle within a Γ_{CRL} interval, i.e., the size of a CRL in each Γ_{CRL} is a constant value with respect to M: $(256 + 256) \times N$, with 256 bits for a pseudonym serial number and 256 bits for its corresponding hash value (excluding an extra byte, the number of remaining pseudonyms in each batch). Fig. 4.b shows that compressing revocation information with a BF could have comparable overhead, i.e., CRL size, with our scheme only if the probability of false positive increases. For example, if $M = 10$, the false positive rate for C^{2}RL scheme should be 10^{-10} to achieve a CRL size comparable to our scheme; otherwise, compressing a CRL with a BF is not as efficient as our scheme. Exactly because each PCA issues multiple pseudonyms in each Γ (for various reasons, e.g., VPKI performance and connectivity) [45], we achieve a significant improvement over C^{2}RL, e.g., 2.6 reduction in CRL size when $M = 10$ and $p = 10^{-30}$.

5.2 Quantitative Analysis

5.2.1 Experimental Setup. We use OMNET++ [8] and the Veins framework to simulate a large-scale scenario using SUMO [14] with a realistic mobility trace, the LuST dataset [21]. For the cryptographic protocols and primitives (ECDSA-256 and SHA-256 as per IEEE 1609.2 [10] and ETSI [26]), we use OpenSSL. V2I communication is IEEE 802.11p[8] [3] and cryptographic protocols and primitives were executed on a virtual machine (dual-core 2.0 GHz).

Placement of the RSUs: To effectively place the RSUs [51], we sorted the intersections with the highest numbers of vehicles passing by. We then placed the RSUs based on these *"highly-visited"* intersections (preferably with non-overlapping radio ranges of RSUs).

Metrics: We evaluate the latency to obtain the latest CRL pieces, i.e., from the time a vehicle enters the system until it successfully downloads them (protocols 2 to 4). We choose a small amount of bandwidth ($\mathbb{B}$) for the distribution, e.g., 10-50 KB/s, in order not to interfere with safety-critical operations. Note that request-triggered CRL piece broadcasts at 10-50 KB/s (80-400 Kbit/s) are practical because 802.11p supports data-rates up to 24 Mbit/s [3].

Table 2 shows the simulation parameters; Tables 3 and 4 show the simulation information for the LuST dataset with respect to different pseudonyms lifetimes (τ_P), revocation rates ($\mathbb{R}$), and maximum bandwidth for distributing CRL pieces ($\mathbb{B}$). We assume that the revocation events are uniformly distributed over a day. For example, if $\tau_P = 60s$, the total number of pseudonyms for one day is around 1.7M. Assuming 1% of the pseudonyms are revoked[9] ($\mathbb{R}$ =1%), there will be around 17K revoked pseudonyms in a day. With our *vehicle-centric* approach, each vehicle only needs to obtain pieces of information for the interval it travels. When $\Gamma_{CRL} = 1$ hour, the average number of entries per Γ_{CRL} is around 710. Assuming $\mathbb{B}$ is up to 10 KB/s, total number of pieces will be 6.[10]

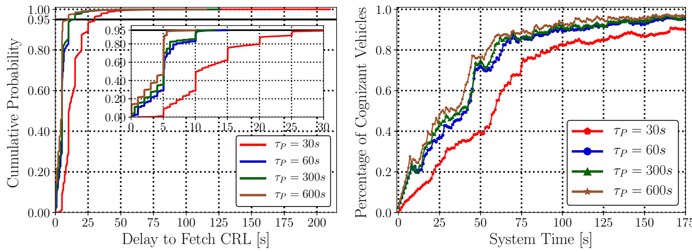
5.2.2 Summary of Results. Our vehicle-centric scheme converges more than 40 times faster than the state-of-the-art [38, 39, 49], termed here the *baseline* scheme, with a similar experimental set up (Fig. 7.b). Moreover, with the baseline scheme, the number of vehicles that successfully downloaded the latest CRL, referred to as *cognizant vehicles*, is highly dependent on the revocation rate and it significantly drops when the revocation rate increases from 0.5% to 5%. However, the performance of our scheme is not affected by the revocation rate: the number of cognizant nodes remains almost intact even if the revocation rate increases up to 5% (Fig. 8). Furthermore, our scheme is more resilient to pollution and DoS/DDoS attacks: with 25% of vehicles in the baseline system compromised, one could prevent almost all legitimate vehicles from obtaining the CRLs; however, with our scheme, the percentage of informed vehicles remains almost intact even if 50% of the vehicles are compromised (Fig. 9). Moreover, our scheme outperforms the baseline scheme in terms of computation overhead: signing and verifying 100 CRL pieces for the baseline scheme require 51 ms and 39 ms, respectively; however, for our scheme, signature and verification delay for 100 CRL pieces is 1 and 12 ms, respectively (Fig. 10.a). Finally, our experiments confirm that our scheme outperforms the baseline scheme in terms of communication overhead, and notably security overhead (Fig. 10.b).

[7]Remark: the two false positive rates mentioned here are different in essence; one is for compressing the CRL entries in C^{2}RL scheme and the another one is for efficiently validating CRL pieces in our vehicle-centric scheme.

[8]Our setup is in-line with the deployment of VC systems, with sparse deployment of RSUs and IEEE 802.1p for safety critical applications [28]. Furthermore, the US Department of Transportation supports Dedicated Short Range Communication (DSRC) to distribute CRL updates (Δ-CRLs), even though a full CRL update cannot be supported as the download time might be longer than the average trip duration [1]. Although Cellular-V2X could be an alternative communication technology, it is not cost-effective (compared to deploying DSRC+Long Term Evolution (LTE)) [1, 9] and it is far behind in the deployment phase [28]. Our experiment is orthogonal to the choice of communication, even though it is envisioned to combine both technologies [11, 28].

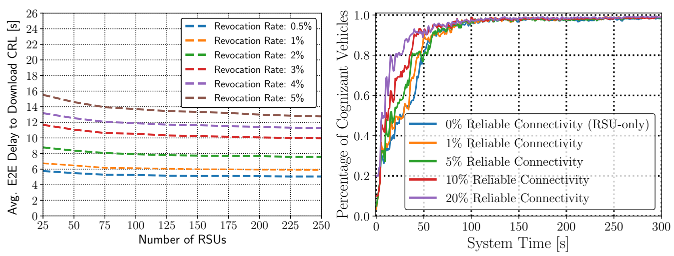
[9]To the best of our knowledge, no statistic is available for the expected percentage of revoked pseudonyms in VC systems. However, "Let's Encrypt", as one of the largest CAs in the Internet, reports around 0.2% of revoked certificates [7]. Note that in VC systems, vehicles are to be provided with multiple, possibly hundreds, of pseudonyms.

[10]These numbers come from the actual implementation of encoded packets. Each CRL piece contains different fields including version, index, total number of pieces in each Γ_{CRL}, and the entries, serialized with the C++ boost library.



(a) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s) **(b) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)**

Figure 5: (a) End-to-end latency to fetch CRL pieces. (b) Percentage of cognizant vehicles over time.



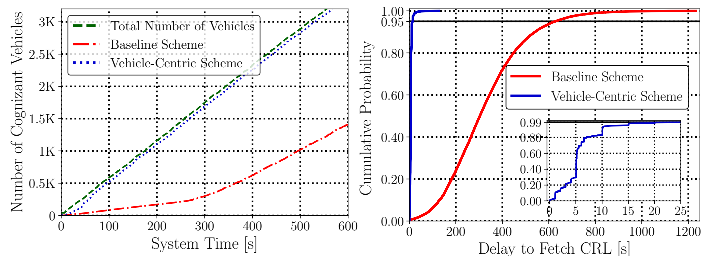
(a) Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s) **(b) Vehicle-centric scheme (TX =5s)**

Figure 6: (a) Average end-to-end delay to download CRLs. (b) Dissemination of CRL fingerprints.

5.2.3 Vehicle-Centric Performance Evaluation. Fig. 5.a shows the CDF of end-to-end latencies to obtain the needed CRL. For example, with $\tau_P = 60s$, 95% of the vehicles received the needed pieces in 15s. Fig. 5.b shows the percentage of cognizant vehicles over time, i.e., those that successfully obtained the CRL pieces. Obviously, the longer the pseudonym lifetime is, the shorter the CRL size is, thus the faster the convergence time becomes. For example, the percentage of cognizant nodes at system time 50 sec, with pseudonym lifetime 30s and 600s, is 39% and 76%, respectively.

Fig. 6.a shows the average end-to-end delay to download the CRL as a function of the number of RSUs for our scheme. The delays were averaged over vehicles operating during the rush hours. The total number of pseudonyms is 1.7M ($\tau_P = 60s$) and the maximum bandwidth to distribute CRL pieces is 25 KB/s. In general, a higher number of RSUs and a lower revocation rate result in a lower average delay to obtain the CRL. For example, the average latency, with $\mathbb{R}$ =1%, decreases from 6.91 to 6.23 as the number of RSUs increases from 25 to 100. As Fig. 6.a shows, leveraging the car-to-car epidemic CRL distribution makes the deployment of a large number of RSUs unnecessary. The optimal number of RSUs to be deployed for a given domain can be properly determined to achieve a certain level of quality of service. Further discussion is beyond the scope of our work.

Fig. 6.b shows how fast a CRL fingerprint is distributed: the signed fingerprint of CRL pieces is periodically broadcasted only by RSUs [60], or they are broadcasted by RSUs (approx. 365 bytes with $TX = 5s$) and, in addition, integrated into a subset of pseudonyms with 36 bytes of extra overhead ($p = 10^{-30}$, $\mathbb{R} = 0.5\%$). Obviously, the distribution of CRL fingerprints with our scheme is faster when there is a small fraction of vehicles with reliable connectivity. However, there is a time lag from the time a PCA releases CRL fingerprints until practically all vehicles are informed about a



(a) 7:00-7:10 am ($\mathbb{B}$ =25 KB/s) **(b) 7-9 am, 5-7 pm ($\mathbb{B}$ =25 KB/s)**

Figure 7: End-to-end delay to fetch CRLs ($\mathbb{R}$ = 1%, τ_P = 60s).

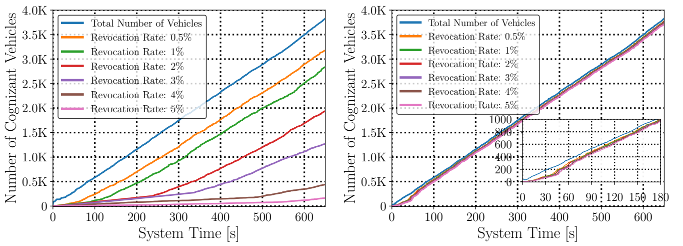
new CRL-update event. Depending on the percentage of vehicles with reliable connectivity and the frequency of revocation events, the PCA could *"predict"* a suitable time to reveal the CRL fingerprint to ensure that every legitimate vehicle operating within the system would receive the CRL fingerprint. For example, the PCA could integrate in a fraction of the recently issued pseudonyms the fingerprint of the current Γ_{CRL} and integrate in another fraction of newly issued pseudonyms the fingerprint of the subsequent Γ_{CRL}.

5.2.4 Performance Comparison. We compare our scheme with the *baseline* scheme [38, 39, 49] that uses RSUs and car-to-car epidemic distribution, with the same assumptions, configuration, and system parameters. For the baseline scheme, the CA signs each CRL piece and can specify a *"time interval"* so that each vehicle receives $\mathbb{D}$ pseudonyms during the pseudonym acquisition process. As a result, for each batch of revoked pseudonyms, a single s_i (256 bit) is disclosed. Similarly, the PCA in our scheme can be configured to issue $\mathbb{D}$ pseudonyms per Γ, i.e., $\mathbb{D} = \frac{\Gamma}{\tau_P}$. To revoke a batch of $\mathbb{D}$ pseudonyms, the serial number of the first revoked pseudonym in the chain and a random number, each 256 bits long, are disclosed. For both schemes, we assume a fully-unlinkable pseudonym provisioning policy [45], i.e., $\Gamma = \tau_P = 1min$.[11]

We further assume that vehicles are provided with enough pseudonyms corresponding to their actual trips for a day. Upon a revocation event, information on all revoked pseudonyms for the day is disseminated for the baseline scheme. In contrast, with our scheme, the CRL entries are distributed in a time prioritized manner, i.e., revoked pseudonyms whose validity intervals fall within the current Γ_{CRL}. Moreover, by disseminating signed BF in advance, the verification cost is minimal compared to baseline signature verification, i.e., zero delay to verify the BF integrated in *fingerprint-carrier* pseudonyms or one signature verification for all CRL pieces.

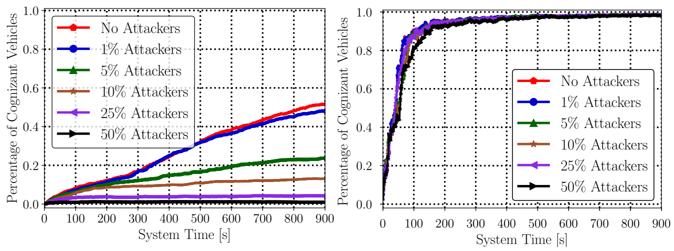
Fig. 7.a shows the number of cognizant vehicles over time for the baseline and our scheme. Vehicle-centric distribution of the CRL pieces converges faster: the number of cognizant vehicles is very close to the actual number of vehicles in the system. Fig. 7.b shows the CDF of delays for the two schemes: for the baseline, $F_x(t = 626s) = 0.95$, whereas with our scheme, $F_x(t = 15s) = 0.95$, i.e., converging more than 40 times faster. The principal reasons for such significant improvements are the prioritization of the revocation entries based on their validity intervals, thus a huge reduction in size, as well as the efficient verification of CRL pieces.

[11] We aim to stress the system with even an impractical configuration. The performance of the two schemes would improve if the system is configured with more conservative parameters, e.g., $\Gamma = 10\tau_P$ (10 pseudonyms per Γ). But we want to ensure that even under the most demanding condition our vehicle-centric scheme remains practical.



(a) Baseline scheme ($\mathbb{B}$ =50 KB/s) (b) Vehicle-centric scheme ($\mathbb{B}$ =50 KB/s)

Figure 8: Cognizant vehicles with different revocation rates.



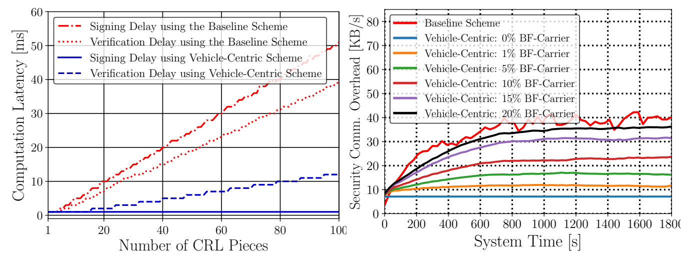
(a) Baseline scheme ($\mathbb{B}$ =25 KB/s) (b) Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s)

Figure 9: Resilience comparison against pollution and DDoS attacks with different number of attackers in the system.

Fig. 8.a shows the number of informed vehicles with different revocation rates ($\mathbb{R}$) for the baseline scheme. The number of cognizant vehicles is highly affected by $\mathbb{R}$: the number of informed vehicles drops by half when $\mathbb{R}$ increases from 0.5% to 3%. Interestingly, the number of cognizant vehicles with $\mathbb{R} = 5\%$ is practically negligible, i.e., the majority of vehicles cannot obtain the CRL pieces within their trip duration because of the huge CRL size. Assume that the total number of pseudonyms is $\mathbb{T}$ and all system configuration parameters are identical. For the baseline scheme, the size of the CRL, $\mathbb{T} \times \mathbb{R}$, linearly increases with $\mathbb{R}$. On the contrary, Fig. 8.b shows that our scheme is *not* affected by $\mathbb{R}$: the number of cognizant vehicles grows as fast as the total number of vehicles in the system. The PCA classifies the revocation entries based on Γ_{CRL} intervals; thus, the size of an *effective CRL* is $\frac{\mathbb{T} \times \mathbb{R}}{|\Gamma_{CRL}|}$, where $|\Gamma_{CRL}|$ is the number of intervals in a day, e.g., $|\Gamma_{CRL}|$ is 24 when $\Gamma_{CRL} = 1$ hour. This results in a huge reduction in CRL size, thus ensuring much faster CRLs distribution.

Fig. 9 shows the percentage of cognizant vehicles when attackers perform pollution and DDoS attacks by periodically broadcasting fake CRL pieces once every 0.5s. Fig. 9.a shows that the baseline scheme is adversely affected once the number of attackers in the system is more than 10% of the vehicles. In contrast, Fig. 9.b illustrates the percentage of cognizant vehicles for our scheme: even if 50% of the OBUs are compromised and misbehave in this way, the percentage of cognizant vehicles is not considerably affected and it still converges within a reasonable delay. Again, such resiliency stems from intelligent partitioning of the CRL, yielding a huge reduction in the CRL size. By integrating the BF of a CRL in the pseudonyms, we achieve an efficient verification of CRL pieces.

Fig. 10.a compares the computation delays for generating and validating CRL pieces for the baseline and our schemes. Signing and verification delays for the baseline scheme linearly increase with the number of CRL pieces. For example, signing and verifying



(a) Computation comparison (b) Communication comparison

Figure 10: (a) Computation latency comparison. (b) Security overhead comparison, averaged every 30s ($\mathbb{R}$=1%, $\mathbb{B}$ = 50KB/s).

100 pieces of CRL require 51 ms and 39 ms, respectively. Depending on the frequency of revocation events and the size of a CRL, this could incur extra overhead for the PCA and the vehicles. But the verification delay for our scheme moderately increases with the number of CRL pieces thanks to the lightweight BF membership validation. The delay to sign the CRL pieces is constant (1 ms), in fact one signature for the BF of pieces to be broadcasted via RSUs and zero additional delay for integrating the fingerprints of CRL pieces to a subset of pseudonyms during the pseudonym acquisition phase; overall, a significant computational improvement is achieved.

Fig. 10.b shows the security overhead due to *signatures* and *fingerprints* for CRL pieces, for the baseline and the vehicle-centric scheme respectively. The ECDSA signature size for the baseline scheme is 72 bytes per piece; the fingerprint in our scheme, 365 bytes long, is signed and it is broadcasted once every 5s via RSUs, and also integrated in a subset of pseudonyms, 36 bytes ($p = 10^{-30}$). Obviously, attaching a pseudonym to every CAM is not practical as the packet overhead increases. To reduce overhead, a pseudonym can be attached to CAMs every α (certificate period) and if there is a pseudonym update process, the new pseudonym is attached every system parameter β (push period) [18]. We configure $\alpha = 10$ and $\beta = 1$ with beaconing frequency $\gamma = 0.1$ (10 CAM/sec) and $\tau_P = 60s$. Fig. 10.b shows that the average security overhead (only the signature field) for the baseline scheme is higher than the one for our scheme, even with 20% of nodes assumed as fingerprint-carriers. Obviously, the longer the pseudonym lifetime, combined with slow neighborhood change, the lower the need to attach pseudonyms, and thus the lower the communication fingerprints overhead. All in all, our scheme outperforms the baseline scheme in terms of computation and communication overhead.

6 CONCLUSION AND FUTURE WORK

We proposed a practical framework to effectively distribute CRLs in VC systems. Through extensive experimental evaluation, we demonstrated that our scheme is highly efficient and scalable, resilient against DoS attacks, and it is a viable solution towards catalyzing the deployment of the secure and privacy-protecting VC systems. As future work, we plan to investigate an optimal interval for Γ_{CRL} based on different factors, e.g., the frequency of revocation events, to guarantee a narrower vulnerability window.

REFERENCES

[1] 2014. V2V Communications: Readiness of V2V Technology for Application. National Highway Traffic Safety Administration, DOT HS 812 014.

[2] 2015. American Community Survey (ACS). http://tiny.cc/hc8qqy.
[3] 2016. IEEE Standard for Wireless Access in Vehicular Environments (WAVE) –Networking Services. *IEEE Vehicular Technology Society* (Jan. 2016).
[4] 2016. When, Where and How Much Motorists Drive. tiny.cc/yinqqy.
[5] 2017. Antpool, The Advanced Bitcoin Mining Pool. antpool.com/.
[6] 2017. Bitmain Antminer S9 Review. http://tiny.cc/12p4qy.
[7] 2017. Let's Encrypt Stats. https://letsencrypt.org/stats/.
[8] 2017. OMNeT++. https://www.omnetpp.org/.
[9] 2018. DSRC Works out Cheaper than Cellular Communications for V2X. http://tiny.cc/qqk4qy.
[10] IEEE 1609.2. 2016. IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. (Mar. 2016).
[11] K. Abboud and et al. 2016. Interworking of DSRC and Cellular Network Technologies for V2X Communications:A Survey. *IEEE TVT* 65, 12 (July 2016), 9457--9470.
[12] M. Amoozadeh. 2012. *Certificate Revocation List Distribution in Vehicular Communication Systems*. Master's thesis. KTH, Stockholm, Sweden.
[13] P. Ardelean and et al. 2009. Implementation and Evaluation of Certificate Revocation List Distribution for VANETs. *Technical Report* (Jan. 2009).
[14] M. Behrisch and et al. 2011. SUMO – Simulation of Urban MObility. In *The 3rd International Conference on Advances in System Simulation*. Barcelona, Spain.
[15] N. Bißmeyer. 2014. *Misbehavior Detection and Attacker Identification in Vehicular Ad-Hoc Networks*. Ph.D. Dissertation. Technische Universität.
[16] Norbert Bißmeyer and et al. 2013. CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs. In *IEEE WONS*. Banff, Canada, 9--16.
[17] Burton H Bloom. 1970. Space/Time Trade-offs in Hash Coding with Allowable Errors. *Commun. ACM* 13, 7 (July 1970), 422--426.
[18] G. Calandriello and et al. 2011. On the Performance of Secure Vehicular Communication Systems. *IEEE TDSC* 8, 6 (Nov. 2011), 898--912.
[19] A-A. Chariton and e al. 2017. CCSP: a Compressed Certificate Status Protocol. In *IEEE INFOCOM*. Atlanta, GA, USA.
[20] J. Clark and et al. 2013. SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. In *IEEE SnP*. Berkeley, USA.
[21] L. Codeca and et al. 2015. Luxembourg SUMO Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research. In *IEEE VNC*. Kyoto, Japan.
[22] D. Cooper. 2000. A More Efficient Use of Delta-CRLs. In *IEEE S&P*. CA, USA.
[23] S. Das and et al. 2004. SPAWN: A Swarming Protocol for Vehicular Ad-Hoc Wireless Networks. In *ACM workshop on VANET*. Philadelphia, PA, USA.
[24] T. Dierks. 2008. The transport layer security protocol version 1.2. (Aug. 2008).
[25] Snowden Era and Bart Preneel. 2015. Cryptography and Information Security in the Post-Snowden era. (May 2015).
[26] ETSI. 2009. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions.
[27] P-T. Eugster and et al. 2003. The Many Faces of Publish/Subscribe. *ACM computing surveys (CSUR)* 35, 2 (June 2003), 114--131.
[28] A. Filippi and et al. 2017. IEEE802.11p Ahead of LTE-V2V for Safety Applications. (Nov. 2017). White Paper. Accessed Date: 20-November-2017.
[29] L. Fischer and et al. 2006. Secure Revocable Anonymous Authenticated Intervehicle Communication (SRAAC). In *ESCAR*. Berlin, Germany.
[30] J. Forné and et al. 2009. Certificate Status Validation in Mobile Ad Hoc Networks. *IEEE Wireless Communications* 16, 1 (Mar. 2009).
[31] D. Förster and et al. 2014. PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks. In *IEEE VNC*. Paderborn, Germany.
[32] D. Förster and et al. 2015. REWIRE–Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks. In *Trust and Trustworthy Computing*. Heraklion, Greece.
[33] C. Gañán and et al. 2012. Toward Revocation Data Handling Efficiency in VANETs. In *Springer Nets4Cars/Nets4Trains*. Vilnius, Lithuania.
[34] C. Gañán and et al. 2013. BECSI: Bandwidth Efficient Certificate Status Information Distribution Mechanism for VANETs. *Hindawi-MIS* 9, 4 (Mar. 2013), 347--370.
[35] C. Gañán and et al. 2013. COACH: Collaborative Certificate Status Checking Mechanism for VANETs. *Network and Computer Applications* 36, 5 (Sep. 2013).
[36] M. Gerlach and et al. 2007. Security Architecture for Vehicular Communication. In *Workshop on Intelligent Transportation*. Hamburg, Germany.
[37] Glenn Greenwald. 2013. NSA Prism Program Taps in to User Data of Apple, Google and Others. tiny.cc/cj4ary.
[38] J-J Haas and et al. 2009. Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET. In *ACM Vehicular Internetworking*. NY, USA.
[39] J-J. Haas, Y-C. Hu, and K-P. Laberteaux. 2011. Efficient Certificate Revocation List Organization and Distribution. *IEEE JSAC* 29, 3 (2011), 595--604.
[40] H-C Hsiao and et al. 2011. Flooding-Resilient Broadcast Authentication for VANETs. In *ACM Mobile Computing and Networking*. Las Vegas, Nevada, USA.
[41] Y. Huang and et al. 2004. Publish/Subscribe in a Mobile Environment. *Wireless Networks* 10, 6 (Nov. 2004), 643--652.
[42] J. Iliadis and et al. 2003. Towards a Framework for Evaluating Certificate Status Information Mechanisms. *Elsevier ComCom* 26, 16 (Jan. 2003), 1839--1850.
[43] M. Khodaei and et al. 2016. Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems. In *IoV/VoI*. Paderborn, Germany.
[44] M. Khodaei, H. Jin, and P. Papadimitratos. 2014. Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure. In *IEEE VNC*. Paderborn, Germany.
[45] M. Khodaei, H. Jin, and P. Papadimitratos. 2018. SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. *IEEE Transactions on Intelligent Transportation Systems* 19, 5 (May 2018), 1430--1444.
[46] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd. In *IEEE VNC*. Torino, Italy.
[47] M. Khodaei and P. Papadimitratos. 2015. The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems. *IEEE VT Magazine* 10, 4 (Dec. 2015), 63--69.
[48] V. Kumar and et al. 2017. Binary Hash Tree based Certificate Access Management for Connected Vehicles. In *ACM WiSec*. Boston, USA.
[49] K-P. Laberteaux and et al. 2008. Security Certificate Revocation List Distribution for VANET. In *ACM VehiculAr Inter-NETworking*. New York, NY, USA.
[50] J. Larisch and et al. 2017. CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers. In *IEEE Symposium on SnP*. San Jose, CA, USA.
[51] Y. Liang, H. Liu, and D. Rajan. 2012. Optimal Placement and Configuration of Roadside Units in Vehicular Networks. In *IEEE VTC*. Yokohama, Japan.
[52] Zhendong Ma and et al. 2008. Pseudonym-on-demand: A New Pseudonym Refill Strategy for Vehicular Communications. In *IEEE VTC*. Calgary, BC.
[53] GF Marias and et al. [n. d.]. ADOPT: A Aistributed OCSP for Trust Establishment in MANETs. In *European Wireless Conference*. Nicosia, Cyprus.
[54] PKI Memo. 2011. C2C-CC. http://www.car-2-car.org/.
[55] S. Micali. 1996. Efficient Certificate Revocation. MIT, MA, USA.
[56] S. Micali. 2002. Scalable Certificate Validation and Simplified PKI Management. In *PKI workshop*, Vol. 15.
[57] M. Mitzenmacher. 2002. Compressed Bloom Filters. *IEEE transactions on networking* 10, 5 (Dec. 2002), 604--612.
[58] T. Moore and et al. 2008. Fast Exclusion of Errant Devices from Vehicular Networks. In *IEEE SECON*. San Francisco, CA.
[59] M. Myers and et al. 1999. *X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP*. Technical Report. RFC 2560.
[60] V-T. Nguyen and et al. 2016. Secure Content Distribution in Vehicular Networks. *arXiv preprint arXiv:1601.06181* (Jan. 2016). Accessed Date: 30-July-2017.
[61] M. Nowatkowski and et al. 2009. Cooperative Certificate Revocation List Distribution Methods in VANETs. In *International Conference on Ad Hoc Networks*.
[62] M. Nowatkowski and et al. 2010. Certificate Revocation List Distribution in VANETs Using Most Pieces Broadcast. In *IEEE SoutheastCon*. Concord, NC, USA.
[63] M. Nowatkowski and et al. 2010. Scalable Certificate Revocation List Distribution in Vehicular Ad Hoc Networks. In *IEEE GLOBECOM Workshops*.
[64] P. Papadimitratos. 2008. "On the road" - Reflections on the Security of Vehicular Communication Systems. In *IEEE ICVES*. Columbus, OH, USA.
[65] P. Papadimitratos and et al. 2006. Securing Vehicular Communications-Assumptions, Requirements, and Principles. In *ESCAR*. Berlin, Germany.
[66] P. Papadimitratos and et al. 2007. Architecture for Secure and Private Vehicular Communications. In *IEEE ITST*. Sophia Antipolis, 1--6.
[67] P. Papadimitratos and et al. 2008. Certificate Revocation List Distribution in Vehicular Communication Systems. In *ACM VANET*. San Francisco, CA.
[68] P. Papadimitratos and et al. 2008. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Comm. Mag.* 46, 11 (Nov. 2008), 100--109.
[69] PRESERVE Project. 2015. www.preserve-project.eu/.
[70] M. Raya and et al. 2006. Certificate Revocation in Vehicular Networks. *Technical Report, EPFL, Switzerland* (2006).
[71] M. Raya and et al. 2007. Eviction of Misbehaving and Faulty Nodes in Vehicular Networks. *IEEE JSAC* (Oct. 2007), 1557--1568.
[72] E. Rescorla and et al. 2012. Datagram Transport Layer Security V.1.2. (Jan. 2012).
[73] G. Rigazzi and et al. 2017. Optimized Certificate Revocation List Distribution for Secure V2X Communications. (2017). Accessed Date: 30-June-2017.
[74] F. Schaub, F. Kargl, Z. Ma, and M. Weber. 2010. V-tokens for Conditional Pseudonymity in VANETs. In *IEEE WCNC*. Sydney, Australia.
[75] Jon A Solworth. 2008. Instant Revocation. In *European PKI*. Trondheim, Norway.
[76] F. Stumpf and et al. 2007. Trust, Security and Privacy in VANETs – a Multilayered Security Architecture for C2C-Communication. *Automotive Security* (Nov. 2007).
[77] S. Tarkoma and et al. 2011. Theory and Practice of Bloom Filters for Distributed Systems. *IEEE Communications Surveys & Tutorials* 14, 1 (Apr. 2011), 131--155.
[78] A. Wasef and X. Shen. 2009. EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad hoc Networks. *IEEE TVT* 58, 9 (2009), 5214--5224.
[79] W. Whyte, A Weimerskirch, V. Kumar, and T. Hehn. 2013. A Security Credential Management System for V2V Communications. In *IEEE VNC*. Boston, MA.