Optimized Certificate Revocation List Distribution for Secure V2X Communications

Giovanni Rigazzi*, Andrea Tassi*, Robert J. Piechocki*, Theo Tryfonas‡, Andrew Nix*
*Department of Electric and Electronic Engineering, University of Bristol, UK
‡Department of Civil Engineering, University of Bristol, UK
E-mail: {g.rigazzi, a.tassi, r.j.piechocki, theo.tryfonas, andy.nix}@bristol.ac.uk

***Abstract*—The successful deployment of safe and trustworthy Connected and Autonomous Vehicles (CAVs) will highly depend on the ability to devise robust and effective security solutions to resist sophisticated cyber attacks and patch up critical vulnerabilities. Pseudonym Public Key Infrastructure (PPKI) is a promising approach to secure vehicular networks as well as ensure data and location privacy, concealing the vehicles' real identities. Nevertheless, pseudonym distribution and management affect PPKI scalability due to the significant number of digital certificates required by a single vehicle. In this paper, we focus on the certificate revocation process and propose a versatile and low-complexity framework to facilitate the distribution of the Certificate Revocation Lists (CRL) issued by the Certification Authority (CA). CRL compression is achieved through optimized Bloom filters, which guarantee a considerable overhead reduction with a configurable rate of false positives. Our results show that the distribution of compressed CRLs can significantly enhance the system scalability without increasing the complexity of the revocation process.**

***Index Terms*—ITS, PPKI, vehicular networks, certificate revocation, Bloom filter, autonomous vehicles.**

I. Introduction

Connected and Autonomous Vehicles (CAVs) rely heavily upon a wide spectrum of heterogeneous technologies combining autonomous driving and vehicle-to-everything (V2X) communications, with the goal of achieving social and economic benefits, such as enhanced road safety, reduced traffic congestion and air pollution [1]. Besides innovative emergency services and infotainment applications leveraging Global Positioning Systems (GPS) and cellular systems, Dedicated Short Range Communications (DSRC) connectivity allows vehicles to exchange real-time information provided by on-board sensor devices, and make decisions based on multiple factors, including road conditions and traffic status [2].

One of the most critical issues concerning the deployment of such vehicular networks is how to efficiently integrate cyber security mechanisms, and ensure trustworthiness and anonymity of exchanged data. Due to the their intrinsic characteristics, V2X communications can be targeted by numerous cyber attacks and security threats, ranging from injection of bogus information or node impersonation, to malicious location tracking and privacy leakage [3]. As a result, security for CAVs has been subject of intensive joint research activities among automotive industry, standardization and regulatory bodies, public authorities and academia, resulting in a plethora of research projects and initiatives across the world [4].

As part of the IEEE 1609 Wireless Access in Vehicular Environments (WAVE) suite, IEEE 1609.2 represents the reference standard for security and privacy adopting a Public Key Infrastructure (PKI), where vehicle authentication is achieved through a Certification Authority (CA) or Trusted Third Party (TPP), in charge of issuing legitimate digital certificates and binding vehicle identity to its public key [5]. An authenticated vehicle can then use its corresponding private key to digitally sign each outgoing packet, whereas sender identity verification is performed by using the public key included in the certificate assigned by the CA. Moreover, the CA is responsible for revoking certificates associated with corrupted or misbehaving entities. To this end, IEEE 1609.2 defines Certificate Revocation Lists (CRL) containing the identities of the revoked certificates, which are periodically updated and disseminated by the CA in the vehicular network [6]. Upon the reception of a new message, a vehicle can identify a legitimate sender by verifying whether the corresponding certificate is not published in the CRL.

To further preserve data privacy and limit vehicle traceability, vehicle identities (VIDs) can be replaced with multiple abstract short-lived identifiers, i.e., pseudonyms, thus realizing a Pseudonym PKI (PPKI) [7]. The pseudonym credentials are issued by the CA, which is also responsible for verifying the eligibility of a vehicle to exchange data by storing its VID. Therefore, location privacy is preserved, as two consecutive messages are signed under two distinct and unlikable pseudonyms. However, this comes at the price of a significant increase in the CRL size, which in turn undermines the scalability and efficiency of the revocation process [8].

In this paper, we propose a low-complexity framework for ensuring trustworthy communications, aiming to reduce the overhead of the CRL distribution via optimized Bloom filter compression. Authors in [6] first adopt Bloom filters to compress the CRLs and reduce the amount of data disseminated. The resulting Compressed Certificate Revocation Lists (C^{2}RL) are then broadcast, while certificate validation is quickly performed by checking the Bloom filter associated with the latest C^{2}RL update. Similarly, [9] proposes the Revocation using C^{2}RL (RC^{2}RL) protocol, where the dissemination of compressed lists is achieved through Road Side Units (RSU) and mobile units. In addition, a quantitative analysis of the protocol performance is presented, showing the existing trade-off between computational complexity and probability of false positives. Bloom filter compression is also employed in [10], where vehicles locally compress and store the list of revoked certificates by generating the revocation keys with the help of optimized CRLs, which are disseminated in a V2V epidemic fashion. However, these solutions do not specify optimal values of the parameters associated with Bloom filters and do not consider the case of multiple certificates assigned to a single vehicle. Differently from the proposed approaches, we aim to evaluate the efficiency of C^{2}RLs in PPKI vehicular networks, and introduce an optimization framework to jointly minimize the filter size and the number of hash functions employed, according to a predefined probability of false positives. Our results show that the CRL distribution process can benefit from the significant overhead reduction, which can be characterized through the compression gain, without causing an increase in complexity. We also demonstrate the C^{2}RLs effectiveness in comparison with a standard CRL approach in a urban setting through large-scale network simulations.

The rest of the paper is organized as follows. Section II describes the network model adopted as well as the certificate compression and the CRL distribution. The proposed optimization framework is illustrated in Section III. In Section IV, we analyze the numerical results obtained, whereas the final conclusions are drawn in Section V.

II. System Model

In this section, we describe the vehicular network and the main entities involved in our system model. We also discuss the fundamental aspects of the C^{2}RL issuance and distribution as well as the procedure to compress the certificates and perform the verification.

A. Network Model

In a typical hierarchical PPKI setup, a Root CA (RCA) coordinates the CAV authentication within a predefined jurisdictional area, such as a city, region, county, etc., by registering vehicles and assigning long-term certificates. Fig. 1 shows the reference scenario considered in this paper. A certain number of Pseudonym CAs (PCA) are also connected to the RCA through wired links, and are responsible for issuing pseudonyms and CRLs. We assume that RCA and PCAs are equipped with sufficient resources in terms of storage and computation, and cannot be compromised by potential attackers. Moreover, the RCA maintains the mapping of short-term credentials to the long-term identity of the vehicles. A number of Road-Side Units (RSU) are deployed along the roads, each connected to a single PCA via a wired backhaul network, while V2I wireless connectivity is achieved by employing DSRC interfaces, such as IEEE 802.11p or ETSI ITS-G5. To mitigate the potential lack of DSRC due to the RSU sparse deployment, we also assume that CAVs are supplied with a cellular radio interface, e.g., 3GPP LTE-A. Although cellular systems introduce additional delay and present limited applicability for safety critical applications, we expect that the integration of these two technologies will represent a key feature of next-generation V2X communications [11]. CAVs sign and broadcast safety-related messages, i.e., Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM), attaching the sender certificate, and are provided with a tamper-resistant Hardware Security Module (HSM) storing the cryptographic material.

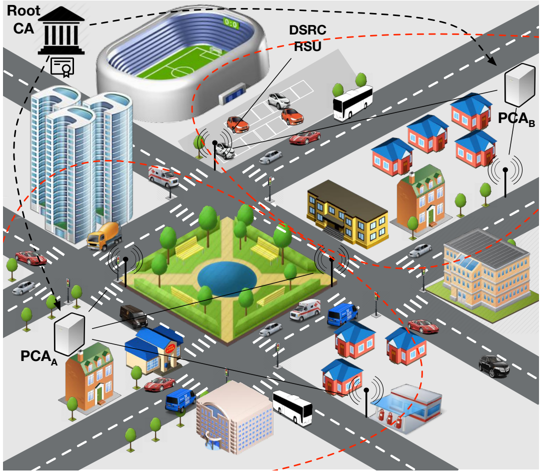

Fig. 1. Illustration of the system model, where two PCAs are connected to a single RCA.

B. Attacker Model

We assume that an internal adversary is able to inject bogus information in terms of fake messages through a legitimate private/public key pair and a related pseudonym certificate. An attacker may also perform a Denial-of-Service (DoS) attack by broadcasting messages with the goal of reducing network resources necessary to reliably exchange safety messages. We assume that anomaly detection algorithms are capable of identifying these threats and triggering the eviction process.

C. Certificate Compression

Following the PPKI approach [12], we assume that each vehicle is assigned a certain number of short-term certificates containing different pseudonyms and pairs of public/private keys. In passive revocation schemes [13], the pseudonym certificate lifetime is minimized, thus vehicles and PCAs need to frequently communicate to initiate the certificate renewal or pseudonym refill procedure. This requirement is usually dictated by the need for minimizing the vulnerability window, i.e., the time between a vehicle is declared illegitimate and subsequent pseudonym refill requests are denied, and all the associated pseudonyms are expired. By contrast, our approach seeks to limit the frequency of pseudonym refills according to the pseudonym change strategy adopted and the storage capability[1]. Efficient compression of CRLs can be accomplished with the help of Bloom filters. A Bloom filter is a probabilistic data structure typically adopted to verify whether a certain element belongs to a set [14]. Such a filter is characterized by a probability of false positives, i.e., probability that an

[1] The problem of how to efficiently change the pseudonyms and determine the change rate is out of the scope of this paper.

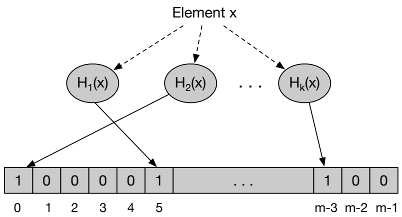

Fig. 2. Example of Bloom filter of size m bits and k hash functions.

element not included in the set is detected due to multiple hash collisions, while false negatives cannot occur. As shown in Fig. 2, a Bloom filter corresponds to a sequence of m bits set to 0. To add an element x, a set of k independent hash functions $H_1, \dots, H_k$ are employed. The output of each hash function matches one of the filter elements and sets to 1 the corresponding bit, while an element previously set to 1 cannot be altered. The verification procedure is then performed by checking the bits corresponding to the output of the hash functions. If all the corresponding bits are set to 1, an element is assumed to be contained in the filter with a certain probability, whereas negative outcomes are always true if at least one of the filter bits is 0. For a target number of filter elements m, the probability of false positives δ is given by [14]:

$$\delta(m,k) \doteq \left[1-\left(1-\frac{1}{m}\right)^{kn}\right]^k, \tag{1}$$

being n the number of elements to add into the filter. Hence, the filter accuracy is influenced by the size, the number of employed hash functions and n, as the larger the set of elements, the higher the probability of obtaining a false positive. Moreover, Bloom filters involve a small amount of computational overhead for insertion and search operations [10].

D. CRL Issuance and Distribution

Every time a misbehaving vehicle is identified, a new CRL needs to be issued and sent to the registered CAVs. As a result, all not expired certificates associated with the evicted vehicle must be revoked, otherwise any pseudonym still valid may be used to sign the outgoing traffic[2]. We also assume that a revocation authority, e.g., a government agency, is in charge of recognizing malicious vehicles and informing the RCA. As shown in Fig. 3, a WAVE CRL consists of *(i)* a header, including a *version* field set to 1, a *signer* field containing information on the CA issuing and signing the CRL, and a *signature* field carrying the signature of the signer, and *(ii)* the unsigned CRL field. A detailed description of each sub-field is reported in [5]. To discuss the differences between a standard CRL (see Fig. 3(A)) and a Bloom filter compressed CRL (see Fig. 3(B)), we focus on the *entries* subfield, containing the identifiers of each revoked certificate. Specifically, in a standard WAVE CRL, each certificate is

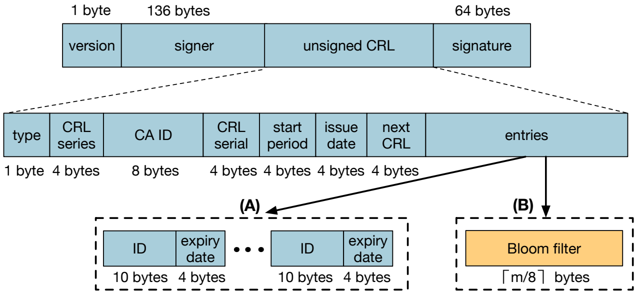

Fig. 3. Structure of a WAVE CRL [5]: standard CRL (A) and C^2RL (B).

identified with an *ID* field and an optional *expiry date* field, used to enhance the efficiency of the certificate storage. By contrast, in our approach, a single Bloom filter of fixed size m bits is carried by the *entries* field. As a consequence, the size of this field remains constant as the number of revoked certificates increases, thus resulting in a significant reduction of the size of the CRLs distributed to the CAVs, as illustrated in Sec. IV. We assume that a C^2RL is issued by the RCA and delivered to its connected PCAs. Next, the RSUs receive the C^2RL forwarded by the PCAs and validate the attached signature. The C^2RL is then signed by the RSU and broadcast to the CAVs through DSRC connectivity, which verify the authenticity and store it in the HSM. Hence, untrustworthy vehicles can be quickly identified by verifying whether the certificates attached in the messages are contained in the filter transmitted in the latest C^2RL. We also point out that only the parameter k needs to be notified to the CAVs in order to fulfill this process, as long as each CAV adopts the same implementation for the k uniformly distributed hashing functions employed. To this end, we consider a single hashing function and provide it with different seed values[3].

Being the generation of false positives inevitable, how to handle vehicle identities wrongly revoked represents an open research question. To overcome this issue, we adopt the approach proposed in [10] and provide the vehicles with a set of *backup pseudonyms* to replace those pseudonyms generating false positives. Each vehicle periodically establishes whether the pseudonym in use triggers a false positive. In other words, each vehicle validates the pseudonym in use against the latest CRL update. Should a legitimate vehicle trigger a false positive, the pseudonym in use is replaced with one of the backup pseudonyms. This entails the provision of additional certificates to compensate for the number of pseudonyms discarded because of false positives. It is worth noting that the resulting false positive probability decreases exponentially as the number of backup pseudonyms per-vehicle increases [10].

III. Proposed Optimization Framework

Let $\mathcal{S} = \{k_1, ..., k_n\}$ be the set of certificates to be added into the Bloom filter, being $|\mathcal{S}| = n$ the cardinality of $\mathcal{S}$. We formulate our filter optimization (FO) model as follows[4]:

[2] This assumption entails linkability among pseudonyms, which limits data privacy. The analysis of the tradeoff between overhead and privacy is left for future work.

[3] In our implementation, the i-th hashing function is simply obtained by setting the corresponding seed value to i.

[4] By $\mathbb{N}$ we denote the set of natural numbers.

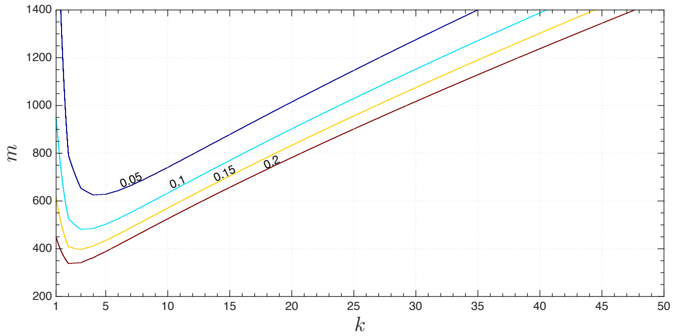

Fig. 4. Contour plot of $\delta(m,k)$, for $n = 10^2$. We only reported the level curves corresponding to the pairs (m,k) where $\delta(m,k)$ is equal to $0.05, 0.1, 0.15$ and 0.2.

$$\text{(FO)} \quad \min_{m,k} \; m \tag{2}$$

$$\text{subject to} \quad \delta(m,k) \leq \hat{\delta} \tag{3}$$

$$k \geq 1, \quad m \geq 1 \tag{4}$$

$$m \in \mathbb{N}, \quad k \in \mathbb{N}. \tag{5}$$

We observe that the FO model carries out a joint optimization of m and k, having as objective the minimization of m, as per (2). Constraint (3) ensures that the probability of false positives is smaller than or equal to a target value $\hat{\delta}$. Obviously, in order for a Bloom filter to exist, it should be at least one bit long and be associated with at least one hash function. These existing constraints are summarized in (4). Finally, constraint (5) imposes m and k to be integer values.

In the attempt of solving the FO model, we relax constraint (5). In addition, we regard the function $\tilde{\delta}(\tilde{m},\tilde{k}) : \mathbb{R}^+ \times \mathbb{R}^+ \to [0,1]$ as the real expansion of $\delta(m,k)$ over the set of positive real values $\mathbb{R}^+$. As such, the relaxed FO (rFO) model can be expressed as follows:

$$\text{(rFO)} \;\; \arg\min_{\tilde{m},\tilde{k}} \left\{ \tilde{m} \;\middle|\; \tilde{\delta}(\tilde{m},\tilde{k}) \leq \hat{\delta} \wedge k \geq 1 \wedge m \geq 1 \right\}. \tag{6}$$

Remark 3.1: From (1), it follows that $\delta(m,k)$ goes to 0 as m tends to infinity, which is not surprising (see Section II-C). Furthermore, from (1), we observe that as m increases, $\delta(m,k)$ cannot increase. Hence, considering constraint (3), the more $\delta(m,k)$ approaches $\hat{\delta}$, the more m is likely to decrease, as also shown in Fig. 4. Obviously, the same observation also applies to $\tilde{\delta}(\tilde{m},\tilde{k})$.

For a given value of $\hat{\delta}$, we define the function $\tilde{m}(\tilde{k})$ providing the value of $\tilde{m}$ such that relation $\tilde{\delta}(\tilde{m}(\tilde{k}),\tilde{k}) = \hat{\delta}$ holds. From (1), $\tilde{m}(\tilde{k})$ can be defined as follows:

$$\tilde{m}(\tilde{k}) \doteq \left[1 - \left(1 - \hat{\delta}^{-\frac{1}{\tilde{k}}} \right)^{\frac{1}{\tilde{k}n}} \right]^{-1}. \tag{7}$$

We denote by $(\tilde{m}^*,\tilde{k}^*)$ the optimum solution of rFO. From Remark 3.1, we observe that the optimum solution of rFO shall satisfy condition $\tilde{\delta}(\tilde{m}^*,\tilde{k}^*) = \hat{\delta}$. As such, the value of $\tilde{k}^*$ can be defined as follows:

$$\tilde{k}^* = \arg\min_{\tilde{k}} \left\{ \tilde{m}(\tilde{k}) \right\}, \tag{8}$$

Procedure 1 Solution of FO

```
1:  $\tilde{k}^* \leftarrow$ the real root of (11)
2:  $\tilde{m}^* \leftarrow \tilde{m}(\tilde{k}^*)$
3:  $i \leftarrow 1$
4:  for $k \leftarrow \lfloor \tilde{k}^* \rfloor, \lceil \tilde{k}^* \rceil$ do
5:      $\mathbf{k}(i) \leftarrow k$
6:      $\mathbf{m}(i) \leftarrow \lfloor \tilde{m}^* \rfloor$
7:      while $\delta(\mathbf{m}(i),\mathbf{k}(i)) > \hat{\delta}$ do
8:          $\mathbf{m}(i) \leftarrow \mathbf{m}(i) + 1$
9:      $i \leftarrow i + 1$
10: for $i \leftarrow 1, 2$ do
11:     if $\delta(\mathbf{m}(i),\mathbf{k}(i)) > \hat{\delta}$ then
12:         $\mathbf{m}(i) \leftarrow NaN$
13:         $\mathbf{k}(i) \leftarrow NaN$
14: if $\mathbf{m}(1) \neq \mathbf{m}(2)$ then
15:     $j \leftarrow$ index of the smallest element in $\mathbf{m}$
16: else
17:     $j \leftarrow$ index of the smallest element in $\mathbf{k}$
18: return $(\mathbf{m}(j),\mathbf{k}(j))$
```

while $\tilde{m}^*$ is simply equal to $\tilde{m}(\tilde{k}^*)$.

From (7), we derive the first order derivative of $\tilde{m}(\tilde{k})$, which is [15]:

$$\frac{\partial \tilde{m}}{\partial \tilde{k}} = \frac{T^{\frac{1}{\tilde{k}n}}}{(1 - T^{\frac{1}{\tilde{k}n}})^2} \left[\frac{\hat{\delta}^{\frac{1}{\tilde{k}}} \log(\hat{\delta})}{\tilde{k}^3 n T} - \frac{\log(T)}{\tilde{k}^2 n} \right], \tag{9}$$

where

$$T \doteq 1 - \hat{\delta}^{\frac{1}{\tilde{k}}}. \tag{10}$$

We observe that the equation $\frac{\partial \tilde{m}}{\partial \tilde{k}} = 0$ has at least a real root iff the equation

$$\hat{\delta}^{\frac{1}{\tilde{k}}} \log(\hat{\delta}) - \tilde{k} T \log(T) = 0 \tag{11}$$

has at least a real root, as well. By resorting to the bisection strategy [16], it is numerically simple to observe that this circumstance occurs for practical values of $\tilde{m}$, $\tilde{k}$ and $\hat{\delta}$[5]. Finally, we observe that the real root of (11), if it exists, is equal to $\tilde{k}^*$.

From the optimum solution $(\tilde{m}^*,\tilde{k}^*)$ of rFO, we derive the optimum solution (m^*,k^*) of FO, as per Procedure 1. In particular, for each value in vector $\mathbf{k} = [\lfloor \tilde{k}^* \rfloor, \lceil \tilde{k}^* \rceil]$, the for-loop at lines 4-9 and 10-13 (of Procedure 1) derives the minimum filter length that meets constraint (3). These values are then stored in vector $\mathbf{m}$. Lines 14-17 allow the procedure to select the solution associated with the smallest filter size or, if both the solutions refer to the same filter size, the procedure returns the one with the smallest number of hash functions.

IV. Performance Evaluation

In this section, we discuss the performance in terms of overhead reduction obtained by employing our optimized framework. To this end, we denote by $\mathcal{G}$ the compression gain,

[5] Specifically, we refer to $\tilde{m} \in [1, 2^{32}]$, $\tilde{k} \in [1, 10^3]$ and $\hat{\delta} \in [10^{-4}, 2 \cdot 10^{-1}]$.

TABLE I
SYSTEM PARAMETERS CONSIDERED IN THE HOLLOWAY SCENARIO.

Parameter	Value	Parameter	Value
Area size	$3\,\mathrm{km} \times 2\,\mathrm{km}$	Max. UDP packet size	1024 bits
Sim. duration	$3600\,\mathrm{s}$	Carrier freq.	$5.89\,\mathrm{GHz}$
SUMO through traffic factor [17]	7	TX power	$20\,\mathrm{mW}$
SUMO traffic count [17]	15	Phy. layer bitrate	$11\,\mathrm{Mbps}$
No. pseudonyms per-vehicle	1000	Sensitivity	$-89\,\mathrm{dBm}$
CRL TX interval	$300\,\mathrm{s}$	Thermal noise	$-110\,\mathrm{dB}$
Optimized Bloom filter	$\hat{\delta} = 10^{-3}$, $n = 300$		

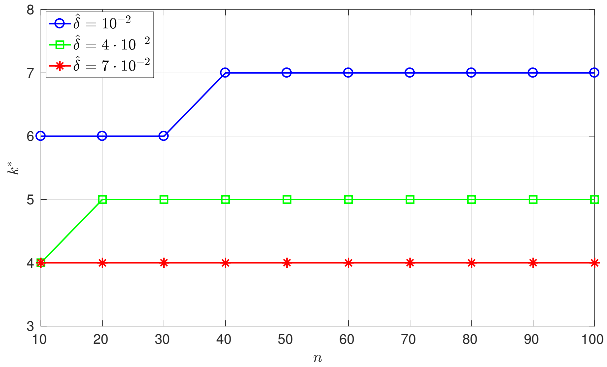

Fig. 5. Optimal number of hash functions k^* for different values of n and $\hat{\delta}$.

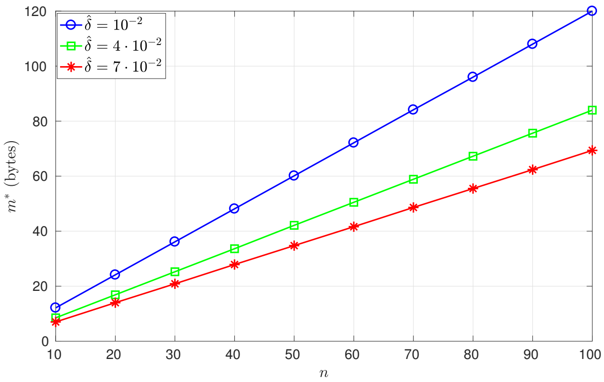

Fig. 6. Optimal filter size m^* for different values of n and $\hat{\delta}$.

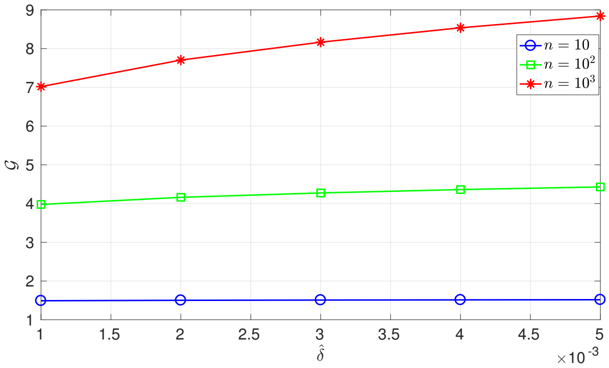

Fig. 7. Compression gain as $\hat{\delta}$ increases and for different values of n.

corresponding to the ratio between the size of a standard CRL and the size of a C^{2}RL adopting the Bloom filter compression. As described in Sec. II-D, a standard CRL consists of a fixed section of 230 bytes and an additional 14 bytes per each revoked certificate, whereas the size of a CCRL is equal to $230 + \lceil m/8 \rceil$ bytes. Finally, we consider a large-scale urban scenario and evaluate the C^2RL gains through network simulations.

A. Optimal Values of k and m

Fig. 5 shows the optimal number of hash functions k^* for different values of $\hat{\delta}$ and varying input load n. As expected, a less strict requirement in terms of false positives leads to a lower and constant k^* as the number of certificates to be compressed becomes higher. On the other hand, by decreasing $\hat{\delta}$ we observe an increment of the optimal number of hash functions, which is necessary to reduce the probability of false positive reports. In addition, Fig. 6 shows the optimal filter size m^* (in bits) to meet different values of $\hat{\delta}$ as a function of n. We note that m^* linearly increases as the input load becomes higher, thus allowing to keep the false positive rate less than or equal to $\hat{\delta}$. Furthermore, the filter size increase becomes more relevant for $\hat{\delta} = 10^{-2}$, as shown by the gap between the blue and green line. This in turn indicates the amount of space required in the filter to prevent multiple hash collisions.

B. C^2RL v.s. Standard CRL

Fig. 7 shows the compression gain $\mathcal{G}$ as $\hat{\delta}$ increases and for different numbers of certificates revoked n. We can note the key benefit provided by the CRL compression, consisting in a significant reduction of the overhead generated by the revocation process. It is also worth pointing out that for low values of n the gain is constant, as the probability of false positives does not significantly influence the choice of the optimal m. By contrast, for higher loads, e.g., $n = 10^3$, we observe that $\mathcal{G}$ increases from 7 to 9, which shows the efficiency of Bloom filters for storing high amounts of certificates as compared with standard CRLs. To analyze the performance of the optimized CRL distribution, we also consider an urban vehicular scenario, where vehicles are distributed on an area of 5 km^2 with different spatial densities, i.e., number of vehicles per km^2, managed by a single PCA. Furthermore, we assume that each vehicle owns a set of 43800 certificates, which corresponds to the fixed amount of certificates requested by a vehicle driving for two hours and every day of the year [18]. Moreover, we define the revocation rate ρ, representing the percentage of vehicles per hour whose certificates must be revoked. Fig. 8 shows the average compression gain over an hour, for different values of ρ as the vehicle density increases, and fixed $\hat{\delta} = 10^{-3}$. We note that for $\rho = 0.1\%$, $\mathcal{G}$ considerably increases in the range of densities between 20 and 40, whereas a saturation effect occurs for values of density higher than 60 vehicles per km^2. This is more evident

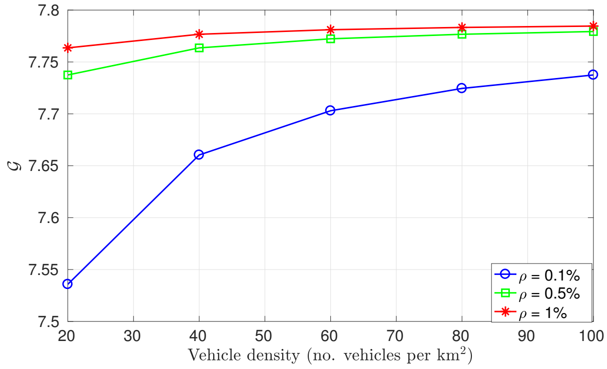

Fig. 8. Compression gain as the vehicle density increases and for different values of ρ ($\hat{\delta} = 10^{-3}$).

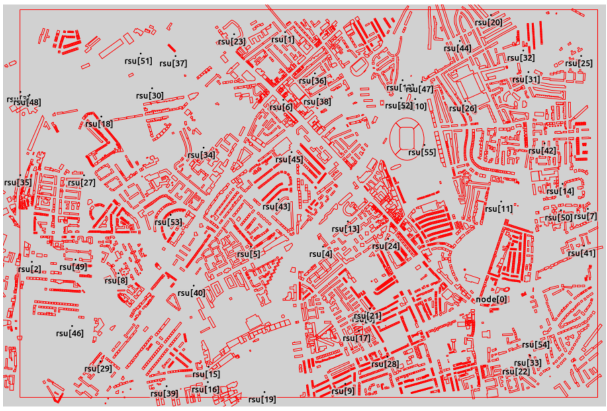

Fig. 9. Map of the simulated area in Holloway (London, UK). The figure shows the footprint of the main buildings present in the area and a possible RSU deployment.

for ρ equal to 0.5% and 1%, where the compression gain immediately reaches a saturation level around 7.78. In other words, for higher values of ρ the filter size needs to increase to meet the $\hat{\delta}$ constraint, while m^* remains low for lower revocation rates.

C. Large-Scale Urban Scenario

To further evaluate the performance gain of the C^2RL scheme over the standard CRL performance, we implemented the aforementioned revocation schemes in a OMNet++ network simulator based on the Veins framework [19]. We considered the urban area of Holloway (London, UK) where a realistic traffic of vehicles has been simulated by means of SUMO [17]. Each vehicle is equipped with a DSRC communication device capable of communicating with RSUs deployed at the side of the road. In order to investigate the impact of different RSU deployments, we placed RSUs uniformly at random in the simulated area preventing the RSUs from being placed within the footprint of a building, as shown in Fig. 9. In particular, we considered scenarios ranging from 28 to 139 RSUs. Periodically, the CA generates a CRL, which is fragmented by the RSUs, encapsulated in UDP packets and transmitted over the DSRC interface. A list of the relevant simulation parameters is reported in Tab. I.

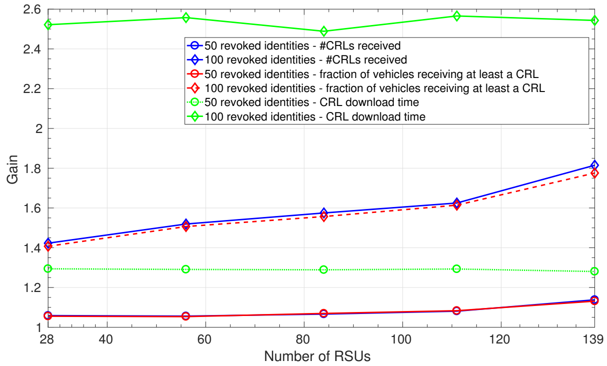

Fig. 10. Gains in terms of CRL delivery ratio, percentage of vehicles successfully receiving a CRL and CRL download time.

Fig. 10 shows the gains achieved employing the C^2RL scheme over a standard CRL approach in terms of total number of CRLs received by all the vehicles, fraction of vehicles receiving at least one CRL, and average CRL download time as a function of the number of RSUs. The derived performance values have been averaged over multiple instances of RSU deployments. We simulated the cases where 50 or 100 vehicles identities per-hours are revoked and each vehicle holds 1000 pseudonyms. We observe that, in the case of the C^2RL scheme, the Bloom filter parameters m and k have been optimized as in Sec. III, by referring to $\hat{\delta} = 10^{-3}$ and a value of n equal to the average number of vehicles present in the simulated area per-second. We note that a higher number of RSUs per-area ensure higher gains for 100 revoked vehicle identities both in terms of the total number of CRLs received by all the vehicles and the fraction of vehicles receiving at least one CRL - thus ensuring, in the case of 139 RSUs, gains greater than 1.55 and 1.6, respectively. These effects are also detectable for 50 revoked identities per-hours, yet limited due to the lower traffic load. From Fig. 10, we also observe that C^2RL guarantees a shorter CRL download time resulting in an average CRL download time gain greater than 2.5, for 139 RSUs and 100 identities revoked per-hour.

V. Conclusions

In this paper, we proposed an optimized framework to streamline the certificate revocation distribution in a PPKI-based vehicular network. We illustrated the scalability issue resulting from the adoption of a large set of pseudonym certificates per each CAV and discussed the benefits of CRL compression through Bloom filters. Significant compression gains can be achieved by adding revoked certificates into a Bloom filter and then disseminating the C^{2}RL in the network. We also investigated the impact of different input loads and false positive rates on the optimal choice of k and m, and compared our approach with a standard CRL distribution scheme in a realistic large-scale scenario.

Acknowledgments

This work is part of the FLOURISH Project, which is supported by Innovate UK under Grant 102582. The authors would like to thank the project collaborators, in particular, Melina Christina, John McCarthy and Ben Miller.

References

[1] Atkins, "Connected & Autonomous Vehicles - Introducing the Future of Mobility," *Tech. Report*, 2016.

[2] K. Zheng, Q. Zheng, H. Yang, L. Zhao, L. Hou, and P. Chatzimisios, "Reliable and efficient autonomous driving: the need for heterogeneous vehicular networks," *IEEE Comms Magazine*, vol. 53, no. 12, Dec 2015.

[3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[4] M. Zhao, J. Walker, and C.-C. Wang, "Challenges and opportunities for securing intelligent transportation system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 96–105, 2013.

[5] "IEEE P1609.2 – Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages," *IEEE*, 2006.

[6] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate revocation in vehicular networks," *Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland*, 2006.

[7] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[8] M. M. E. A. Mahmoud, J. Mii, K. Akkaya, and X. Shen, "Investigating Public-Key Certificate Revocation in Smart Grid," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 490–503, Dec 2015.

[9] 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*, vol. 25, no. 8, pp. 1557–1568, 2007.

[10] 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, 2011.

[11] K. Abboud, H. Omar, and W. Zhuang, "Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2016.

[12] M. Khodaei and P. Papadimitratos, "The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, 2015.

[13] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*. IEEE, 2008, pp. 1–5.

[14] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, "Theory and practice of bloom filters for distributed systems," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 131–155, 2012.

[15] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*. Elsevier, 2007.

[16] R. Moore, *Methods and Applications of Interval Analysis*, ser. Studies in Applied and Numerical Mathematics. SIAM), 1979.

[17] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO–Simulation of Urban Mobility: An Overview," in *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[18] M. E. Nowatkowski, J. E. Wolfgang, C. McManus, and H. L. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*. IEEE, 2010, pp. 380–383.

[19] "Veins - Vehicle Network Simulation (http://veins.car2x.org/)."