SRPV: A Scalable Revocation Scheme for Pseudonyms-based Vehicular Ad Hoc Networks

Khaled Rabieh[1], Miao Pan [2], Zhu Han [2], and Vitaly Ford[3]

[1]Department of Computer Science, Sam Houston State University, Huntsville, TX, USA
[2]Electrical & Computer Engineering Department, University of Houston, Houston, TX, USA
[3]Department of Mathematics & Computer Science, Arcadia University, Glenside, PA, USA

***Abstract*—The cryptographic credentials of misbehaving vehicles should be revoked in a timely manner to prevent jeopardizing the network. However, the revocation is a challenging problem in VANETs because of its stringent privacy requirements and the large network scalability. Each vehicle receives a large number of unlinkable certified pseudonyms to protect privacy. Large storage and computation are required to store the revocation list and verify the authenticity of messages, respectively. In this paper, we propose a scalable revocation scheme that reduces the revocation list storage overhead and the revocation checking delay in pseudonym-based VANETs. The revocation of vehicle's credentials is achieved by adding a single trapdoor in a revocation list. The vehicles use the published trapdoors for revocation check by computing simple operations instead of sequentially searching a large set of pseudonyms. Chameleon hashing is used to generate the pseudonyms and revoke them if needed. Using computationally efficient multi-signature, vehicles can cooperatively vote to revoke the credentials of a misbehaved vehicle. The objective of using multi-signature is to increase the creditability of revocation requests. Our experiments and extensive evaluations show that our scheme can revoke a large number of pseudonyms with minimum storage and computation overhead.**

Keywords: Revocation schemes, privacy preserving, Chameleon hashing, multi-signature, trapdoor and VANETs.

I. Introduction

Vehicular Ad Hoc Networks (VANETs) are an emerging technology that is expected to have promising results in better driving experience and infotainment applications [1]. Privacy is very crucial part in these networks because drivers may be reluctant to use VANETs if they feel that their privacy is jeopardized. One way to achieve privacy is by providing vehicles with a large number of forged identities that reveals nothing about the real identity of the driver which are called pseudonyms [2], [3]. One condition for pseudonyms to protect individual's privacy is that they should not be linked [1]. Linking pseudonyms abolishes its objective in protecting privacy because an attacker can collect a sufficient number of them and link them to a single identity/driver. Later, the attacker can disclose the real identity of the driver from the driver's activity such as the visited locations and the time spend at specific locations. Pseudonyms are issued by a trusted party periodically over long time intervals, e.g., every one to three years. Therefore, the number of pseudonyms required by one vehicle is sufficiently large to preserve its privacy in a long time period. For example, 43,800 is the estimated number of pseudonyms to be consumed by a vehicle in one year if pseudonyms are changed every minute for two hours driving duration every day according to [4], [5].

The revocation has been extensively studied in different networks such as smart grid and VANETs. The objective of revocation is to stop a misbehaved node/attacker to jeopardize the network by publishing revocation information. The published revocation information is used by other vehicles to check if a node is revoked or not. Intuitively, the revocation schemes can be classified into centralized and decentralized network models [6]. In centralized schemes, Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) are used to publish the revocation information. In the VANET context, the CRL size grows linearly with the increment of revoked vehicles [7]. This large increase of the CRL size due to a large number of pseudonyms should be added when revoking a single vehicle [8]. In [2], it is shown that an additional information of one MByte in size should be added to revoke one vehicle. In [8], the average number of revoked pseudonyms is estimated to be 1.37×10^{12} in US only based on statistics by the US National Transportation. In decentralized revocation schemes, the vehicles do not need to contact a centralized authority to revoke an attacker's credentials. But, a group of vehicles can revoke a misbehaved node using a secret key shared among them. However, the vehicles still need to contact the Certificate Authority (CA) for generating new secret keys to exclude the revoked vehicle.

In this paper, we propose a Scalable and computationally efficient Revocation scheme for Pseudonyms-based VANETs (SRPV) to meet the privacy requirements of such networks. Specifically, SRPV allows drivers to use a large number of certified pseudonyms to preserve their privacy while the revocation of misbehaved vehicles' credentials is achieved with minimum communication and computation overhead. Instead of adding a large number of pseudonyms to the CRL, the CA needs to append a single fixed-size trapdoor. The trapdoor

The research of M. Pan is partially supported by US NSF CNS-1350230 (CAREER), CNS-1702850, CNS-1646607, and CNS-1343361.

Z. Han is with the University of Houston, Houston, TX 77004 USA (e-mail:zhan2@uh.edu), and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea. The research of Z. Han is partially supported by US NSF CNS-1717454, CNS- 1731424, CNS-1702850, CNS-1646607,ECCS-1547201,CMMI-1434789,CNS-1443917, and ECCS-1405121.

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

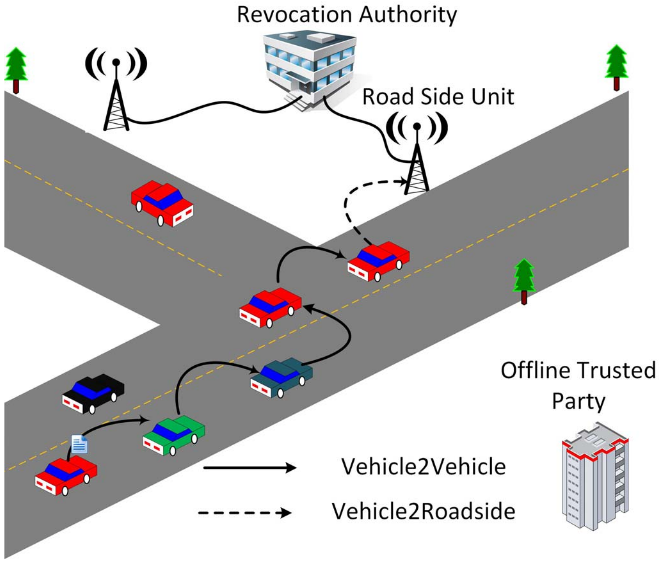

Fig. 1: Our Network Model.

is used to check the revocation status instead of sequentially searching a large revocation list which is a time consuming process. Our objective is not only to reduce the size of the CRL, but to minimize the computation overhead carried out by the vehicles, which needs to verify a large number of messages in short period of time. Using the proposed scheme, the transmission delay of the CRL is reduced, and hence the attackers can not take advantage of the long revocation window to compromise VANETs.

In [9], short group signatures are proposed with an efficient verifier-local revocation technique. The revocation is achieved by publishing the secret key of the group member to the CRL. Our work is different from [9] in the following aspects. a) SRPV supports pseudonym-based privacy preserving schemes which are compatible and can be used with any type of signatures and not only group signatures. b) The group signature generation, verification and length have much more overhead than other types of signatures with the same order. For example, the length of group signature is estimated to be 1,192 and 1,536 bits in [9] and [10], respectively. But, it only requires 171 bits using the signature scheme in [11] which can be used to sign pseudonyms in the proposed scheme, *given that both signatures have the same security level.*

The remainder of the paper is organized as follows. In Section II, the network and threat models are described. We discuss some preliminaries in Section III. Our scheme is presented in Section IV. Performance evaluations are explained in Sections V. Finally, Section VI discusses the related works and Section VII concludes the paper.

II. Network and Threat Models

A. Network Model

As shown in Fig. 1, the network model consists of four entities.

- **Offline Trusted Party** (OTP): The OTP is a centralized authority that is responsible for generating the secret keys and credentials for the vehicles. It is offline because our scheme can run without the need to constantly contacting it.
- **Road Side Units**: RSUs are access points that are deployed on roads. They are connected to the RA via a fast wired communication technology, e.g., wired cables, 4G. RSUs act as a bridge between the vehicles and the RA in essence that the RA distributes the CRL to vehicles through the RSU. Vehicles send revocation requests to the RA through the RSUs as well.
- **Vehicles**: The network consists of a large number of vehicles. They communicate with each other and with RSUs distributed on the roads using IEEE 802.11p standard. Vehicles contact the OTP to receive the necessary credentials which are a group of certified pseudonyms and public/private key pairs.
- **Revocation Authority** (RA): The RA revokes the credentials of misbehaved vehicles. The RA receives revocation requests from vehicles and revoke the credentials of the attacker. There is a fast and reliable wired link between the RA and the RSUs to enable timely and efficient revocation procedure.

B. Adversary and Threat Model

The OTP and the RA are trusted, operated by the government and can not be compromised. The RSUs are devices deployed on roads and we do not trust to keep secret keys/credentials inside them. Most of the vehicles are honest in the sense that they do not disrupt how our scheme runs or the communications between entities. Moreover, they report a misbehaved vehicle to the RA in case they witness an attack to the network. However, some of vehicles may misbehave or attempt to attack the network, i.e., disseminate wrong information or drop packets. Such attackers need to be revoked in a timely manner to limit the harm they can cause to VANETs.

III. Preliminaries

In this section, we explain some of the basic techniques that will be used in our scheme.

A. Chameleon Hashing

Chameleon hashing is a one-way hash function h that is used to compute a message digest similar to other hash functions. It is a collision resistent function, but using a trap door, collisions for any input can be easily computed. Every user has a pair of keys (p_k,s_k). The public key p_k and a random element r are used to compute the hash $h = h(m, r)$. s_k is the trap door and should be kept secret. In order to compute collisions, an algorithm takes s_k, m and r as an input and outputs $\acute{m}$ and $\acute{r}$ where $h(m, r)$ = $h(\acute{m}, \acute{r})$.

When combined with digital signatures, it can achieve non-repudiation and non-transferability, i.e., the issued signature cannot be validated by another party without the consent of the signer. The verifier of the signature does not accept it since the user with the trap door s_k is able to generate the same proof by himself. Voting scheme is an example of applications that use chameleon hashing where it requires certain parties only to verify the signature. The voting center can prove to the user that his vote is counted *(i.e., by signing on the chameleon hash of his vote)* without letting him able to prove to a third party that he votes for a certain party. In our scheme, we use chameleon hash to revoke the vehicles' pseudonyms in case of misbehavior detection. This is achieved by publishing the trapdoor in the revocation list.

B. Multi-Signatures

In multi-signature, a group of users of size n can sign a message m in cahoots and generate a single signature instead of generating n signatures. The multi-signature is characterized by small signature verification time and minimum signature size which is very efficient when compared with traditional signatures. This signature is used in web wallets and co-payment where multiple users have the authority to spend a certain amount of e-cash. The e-wallet server approves the spending of an amount of money if all users agree and *sign* to spend this amount. It is used in VANETs to increase the creditability of distributed traffic events. This is because vehicles tend to believe a message sent from many vehicles more than a message sent from only one vehicle. Let G_1 and G_2 be additive and multiplicative cyclic groups, respectively. The order of G_1 and G_2 is q where q is a large prime number. Let Z_q be a finite field of order q. There exists an admissible bilinear pairing $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ that maps elements from G_1 to G_2. We use the multi-signature scheme in [12] which is based on bilinear pairing with the following four properties.

- **Computability**: An efficient algorithm exists to compute $\hat{e}(g_1, g_2)$ for all g_1, $g_2 \in G_1$.
- **Bilinearity**: $\hat{e}(ag_1, bg_2) = \hat{e}(g_1, g_2)^{ab}$ for all g_1, $g_2 \in G_1$ and a, $b \in Z_q$.
- **Non-degeneracy**: There exist g_1, $g_2 \in G_1$ such that $\hat{e}(g_1, g_2) \neq 1$.
- **Symmetricity**: $\hat{e}(g_1, g_2) = \hat{e}(g_2, g_1)$ for all g_1, $g_2 \in G_1$.

Multi-signature is used to revoke the credentials of an attacker in this scheme. A group of vehicles vote by signing on the pseudonym of the attacker to convince the revocation authority of occurrence of misbehavior.

IV. Scalable Revocation Scheme for Pseudonyms-based VANETs (SRPV)

In this section, we discuss the system bootstrap, the revocation procedure and the modified revocation check.

A. Bootstrap

The OTP generates two additive and multiplicative groups G_1, G_2, respectively, have the same prime order q. The generators of G_1 and G_2 are P and g, respectively. Let Z_q be a finite field of order q. The master secret key s is chosen randomly from Z_q. The public key is $Q = sP$. H_1 is a cryptographic one way hash function such that $H_1 : \{0,1\}^* \rightarrow G_1$. Let H_c be a chameleon hash function such that $H_c : \{0,1\}^* \rightarrow \{0,1\}^l$ where l is the length of the output. The OTP publishes the public parameters of the system $\{G_1$, G_2, $\hat{e}$, P, g, q, Q, H_1, $H_c\}$ and keeps s secret. For each vehicle v, the OTP chooses a random element $x \in Z_q$ which is a per-vehicle secret. To generate one pseudonym, it chooses two random elements r, $m \in Z_q$ and computes $H_c(r, m) = g^{m+xr} = g^m \times g^{xr}$. The pseudonym consists of the pair $\{g^m$, $g^r\}$. In order to compute the next pseudonym, the OTP chooses two elements $\hat{r}, \hat{m} \in Z_q$ that satisfies the equation $mx + r = \hat{m}x + \hat{r}$. The process is repeated until the OTP generates a sufficient number of pseudonyms. The OTP signs every pseudonym p_i using the secret key s and generates the corresponding certified pseudonym by computing the signature $\sigma = sH_1(p_i)$. The vehicle receives the pseudonyms list during its periodic registration. The per-vehicle secret key x and the corresponding pseudonyms list are sent to the RA.

B. Revocation Procedure

When a vehicle suspects an attack or a misbehavior from a certain vehicle, it composes *a revocation request packet*. There are many attacks that can be detected by a driver such as a selfish behaviour, Sybil attack and much more. For example, if a certain vehicle is proven to broadcast falsified events such as a fake accident or traffic incident. An initiator vehicle A starts the revocation procedure by singing a revocation request packet. The revocation request Req contains the pseudonym p_r of the attacker to be revoked, the revocation reason, time stamp TS, the signature δ_a and the digital certificate $cert_a$. A randomly chooses $r_a \in Z_q$ and computes the signature δ_a = (S_a, T_a) where $S_a = r_a H_1(Req) + sH_1(Ps_a)$, $T_a = r_a P$ and Ps_a is a pseudonym belongs to A. Then, A broadcasts the revocation request Req and the signature δ_a to all vehicles in its vicinity. Any vehicle can verify the authenticity of the revocation request by checking if $e(S_a, P) \stackrel{?}{=} e(T_a, H_1(Req))e(Q, H_1(Ps_a))$. The verification of the revocation request succeeds if and only if A uses its private key $sH_1(Ps_a)$ to sign the message because

$$\begin{aligned} e(S_a, P) &= e(r_a H_1(Req) + sH_1(Ps_a), P) \\ &= e(r_a H_1(Req), P)e(sH_1(Ps_a), P) \\ &= e(H_1(Req), P)^{r_a} e(H_1(Ps_a), P)^s \\ &= e(H_1(Req), r_a P)e(H_1(Ps_a), sP) \\ &= e(H_1(Req), T_a)e(H_1(Ps_a), Q) \\ &= e(T_a, H_1(Req))e(Q, H_1(Ps_a)). \end{aligned}$$

C. Anonymous Voting and Revocation Check

After the verification succeeds, if a vehicle B agrees to revoke the vehicle and needs to increase the creditability of the revocation request, it aggregates its signature to the signed revocation request using multi-signature. Similar to A's signature, B generates its own signature (S_b, T_b) on the same revocation request Req where $S_b = r_b H_1(Req) + sH_1(Ps_b)$ and $T_b = r_b P$ where $r_b \in Z_q$ and Ps_b is B's pseudonym. Then, it computes the aggregated signature by simply adding them such that $S_{a+b} = S_a + S_b$ and $T_{a+b} = T_a + T_b$. For aggregating n signatures on a single revocation request, the vehicle computes $S_n = \Sigma_{i=1}^n S_i$ and $T_n = \Sigma_{i=1}^n T_i$. The revocation request packet should be sent after signing it by a threshold number of vehicles which is a configurable network parameter. There is a trade off between creditability and revocation efficiency. The more the number of signatures on a single revocation request the more creditable the request is. However, this brings an additional cost of processing delay of the the revocation request since more signatures need to be aggregated.

When a sufficient number of vehicles signs the revocation request, the request $\{S_n, T_n\}$ is sent to the RA through the RSU. The RA verifies the multi-signature (S_n, T_n) by checking if $e(S_n, P) \overset{?}{=} e(T_n, H_1(Req))e(Q, \Sigma_{i=1}^{n} H_1(Ps_i))$ where n is the number of vehicles that jointly signed the request. The verification of the multi-signature held by the RA holds because

$$\begin{aligned} e(S_n, P) &= e(\Sigma_{i=1}^{n} S_i, P) \\ &= e(\Sigma_{i=1}^{n}(r_i H_1(Req) + sH_1(Ps_i)), P) \\ &= e(\Sigma_{i=1}^{n} r_i H_1(Req), P) e(s\Sigma_{i=1}^{n} H_1(Ps_i), P) \\ &= e(\Sigma_{i=1}^{n} r_i P, H_1(Req)) e(\Sigma_{i=1}^{n} H_1(Ps_i), sP) \\ &= e(T_n, H_1(Req)) e(\Sigma_{i=1}^{n} H_1(Ps_i), Q) \\ &= e(T_n, H_1(Req)) e(Q, \Sigma_{i=1}^{n} H_1(Ps_i)). \end{aligned}$$

If the verification succeeds, the RA looks up for the secret key x_r which is corresponding to the pseudonym P_r contained in the revocation request. It appends x_r and $\{g^{m_r + x r_r}\}$ to the revocation list, signs the new revocation list and publishes the updated list to be accessible by the vehicles. By adding only one entry in the revocation list, all the pseudonyms of the misbehaved vehicle are revoked. This is because when a vehicle attempts to verify a message signed by a pseudonym $\{g^m, g^r\}$ and instead of sequentially searching the revocation list, the vehicle uses every entry $\{x_r, g^{m_r}, g^{r_r}\}$ in the CRL to compute $g^{m x_r} \times g^{r_r} = g^{m x_r + r_r}$. Then, it checks if $g^{mx+r} \overset{?}{=} g^{x_r m_r + r_r}$. If the check holds and both sides are equal, the pseudonym is considered revoked and the message should be immediately rejected. Otherwise, it proceeds to check the next entry using the same procedure until all the entries in the revocation list are checked. It is clear that a single entry in the revocation list corresponds to revoking one vehicle which is more efficient than adding thousands of attackers' pseudonyms to the list. This decreases the size of the revocation list and more efficient in terms of computation overhead. This is because the verifier computes one exponentiation and multiplication operations instead of sequentially searching a large list of pseudonyms.

V. Performance Evaluations

A. Communication Overhead

Voting for Revocation: The size of the elements of G_1, G_2 is 32 bytes using an order of 256 bits. Accordingly, the size of the signature $\delta_a = (S_a, T_a)$ is 64 bytes since S_a and T_a are both elements in G_1. The revocation reason and the certificate sizes are estimated to be 50 and 100 bytes, respectively. The pseudonym $P_r = \{g^m, g^r\} \bmod q$ is 64 bytes and the time stamp requires 8 bytes. The size of the revocation request is 64 + 50 + 100 + 64 + 8 = 286 bytes. When n vehicles aggregate their signatures and generate $S_n = \Sigma_{i=1}^{n} S_i$ and $T_n = \Sigma_{i=1}^{n} T_i$ on the same request, the aggregated signature has the same size of only one signature since $\Sigma_{i=1}^{n} S_i$ and $\Sigma_{i=1}^{n} T_i$ are elements in G_1. The communication overhead of aggregating an additional signature is 100 bytes which is the certificate size. It is clear that the proposed voting scheme can scale up when more vehicles need to aggregate signatures on a revocation request.

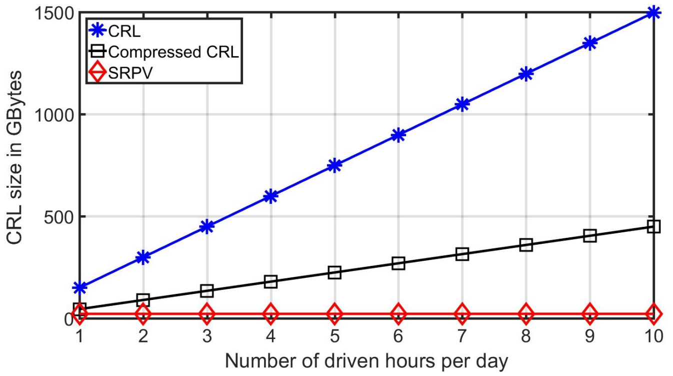

Fig. 2: A comparison between the sizes of the conventional CRL, compressed CRL and the revocation information of SRPV.

Revocation List size: Assuming a vehicle is equipped with pseudonyms sufficient for one year and the average duration of driving is two hours per day, 43,800 pseudonyms should be generated and installed in each vehicle. In [8], the size of one pseudonym to be added to the CRL in case of revocation is estimated to be 14 bytes. In average, if a vehicle has to be revoked after six months, *half the duration of periodic registration*, we need to add $\frac{43{,}800}{2}$= 21,900 pseudonyms to the CRL per revoked vehicle. Consequently, the storage space needed to store these revoked pseudonyms = 14 × 21,900 ≈ 300 Kbytes per vehicle. Even with compressing the CRL with compression ratio of 70% which is a very high compression ratio, it requires 90 Kbytes per vehicle.

In Fig. 2, we compare the sizes of the conventional CRL, compressed CRL and SRPV with respect to the number of driving hours per day. We vary the number of hours driven per day between 1 and 10 hours and we fix the number of revoked vehicles to be 1 million. The CRL size is computed by multiplying 14 × Average number of revoked pseudonyms per vehicle × Number of revoked vehicles. We estimate the average number of revoked pseudonyms per vehicle to be 10,950 × Number of hours driven per day. In SRPV, an entry in the list is dependent on the order of Z_q. Using an order of 256 bits, one entry in the revocation list requires 3 × 256 bits = 96 bytes *to add* $\{x, g^m, g^r\}$. From Fig. 2, when the number of driven hours increases, the CRL size increases linearly because a larger number of pseudonyms is issued to every vehicle. Consequently, this requires more pseudonyms to be added to the list in case of revoking a misbehaved vehicle. It is clear that SRPV offers much less size than that of the conventional CRL even after compression. An interesting fact is that SRPV size is independent from the number of driven hours per day and has fixed size of CRL ≈ 94 MBytes. This is because it is enough to add only one entry *(any pseudonym that belongs*

TABLE I: Computational overhead

Operation	Computation time in ms
Elliptic Curve Pairing	1.5
Elliptic Curve Point Multiplication	0.59
Elliptic Curve Point Addition	0.2
Elliptic Curve Point Double Multiplication	0.79
Modular Exponentiation	0.3
Modular Multiplication	0.1

to the vehicle to be revoked) to revoke all the pseudonyms of a misbehaved vehicle regardless the number of pseudonyms it possesses.

B. Computation Overhead

Voting for Revocation: We show the computation times of the required operations used throughout the SRPV scheme in Table I using an Elliptic Curve of order 256 bits. We use the MIRACL Cryptographic benchmark [13] running on a virtual machine with processor 3.50GHz, Intel Xeon i7-6700 and 2 GB RAM. To generate a signature $\{S_a,\, T_a\}$, it requires to compute double multiplication and multiplication operations, respectively, which takes 0.79 + 0.59 = 1.38ms. In order to aggregate a signature, B performs two point additions operations to add its own signature $\{S_b, T_b\}$ to $\{S_a, T_a\}$, respectively. This requires 2 × 0.2 = 0.4ms. In addition, B has to sign on the revocation request which takes 1.38ms. The total time to aggregate the two signatures = 1.38 + 0.4 = 1.78ms. In order to verify an aggregated signature, the vehicle needs to compute three pairing and n point addition operations where n is the number of vehicles which jointly signs the revocation request. For example if n = 5, it requires a vehicle (5 × 0.2) + (3 × 1.5) = 5.5ms to verify the aggregated signature.

Revocation List Search Time: We setup an experiment using Visual C# to simulate the sequential search operation in large CRLs. Our implementation measures the average search time for a revoked and a valid pseudonym against CRL, respectively. We use different sizes of the CRLs that have 250,000, 500,000, 1M, 2M, 4M, and 5M different revoked pseudonyms *(M stand for million)*. We generate random and unique serial numbers of 14 bytes in length and add them to a revocation list. To search for a revoked pseudonym, a pseudonym is chosen randomly from the list and then a sequential search algorithm is run to look up this pseudonym.

In order to search for a valid pseudonym, we generate a random pseudonym that does not belong to the list. In both cases, we measure the execution time using the Stopwatch class. Our experiment is averaged over 30 runs. To measure the search time in SRPV, the index where a pseudonym is found is divided by the number of pseudonyms per vehicle × 0.4. This is because we only add one entry per vehicle in the CRL in case of SRPV. 0.4 ms is the time needed to compute $g^{mx_r} \times g^{r_r}$ given $\{x_r,\, g^{m_r}, g^{r_r}\}$ which requires one exponentiation and multiplication operations. We consider two cases SRPV-21900 and SRPV-32850 where the revoked pseudonyms per vehicle in the CRL are 21,900 and 32,850, respectively. This is equivalent to revoking misbehaved vehicles after half and quarter of the periodic registration period.

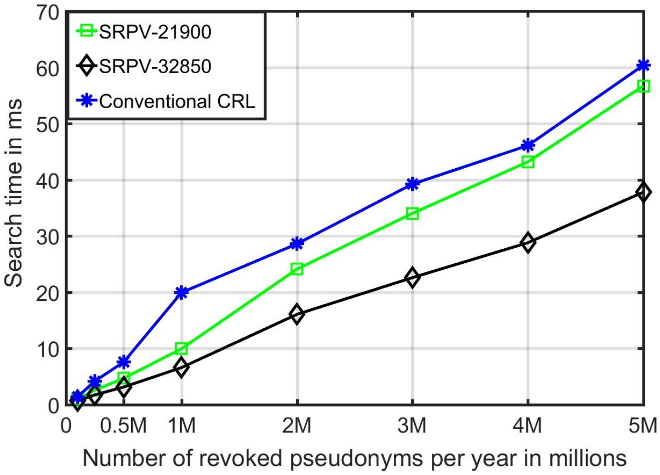

Fig. 3: Average search time for a revoked pseudonym.

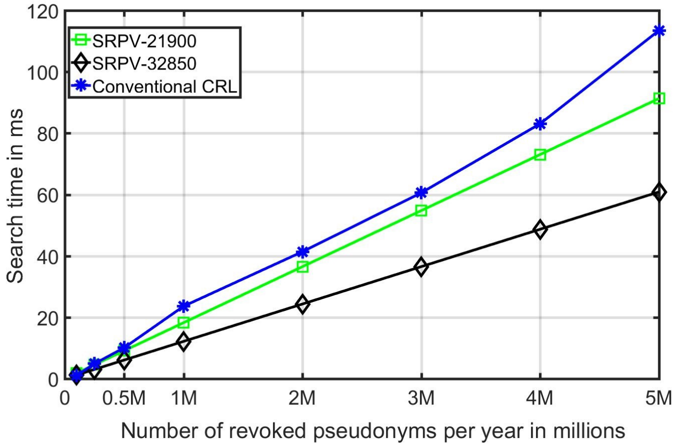

Fig. 4: Average search time for a valid pseudonym.

Fig. 3 depicts the time required for searching a revoked pseudonym using SRPV and the conventional CRL. SRPV requires less search time than the conventional CRL in the two cases. For example, it requires 70ms to search for a revoked pseudonym in a 3M pseudonyms CRL, but, it requires only 22ms to search for the same pseudonym using SRPV-32850. Comparing SRPV-21900 and SRPV-32850, it is shown that when the number of pseudonyms per vehicle increases, the search time decreases. This is because SRPV-32850 requires less pseudonyms to be added to the CRL than SRPV-21900, and hence less computational operations are needed to compute $g^{mx_r} \times g^{r_r}$ for each vehicle.

Similarly, we compute the time required by our scheme to search for a valid pseudonym. Fig. 4 depicts the time required to search for a valid pseudonym and compares between SRPV and the CRL. Searching for a valid pseudonym implicity means iterating through the entire list since the valid pseudonym is not included in the CRL. Obviously, the search time in Fig. 4 is more than that of Fig. 3 for the same number of pseudonyms in the CRL because it requires more time to iterate through the whole list. It is clear that SRPV requires less time than the CRL especially when its size increases. SRPV offers less computation overhead when the number of comparisons operations is very large, and hence it can scale up with large CRLs. The sequential search is faster than SRPV when the number of entries in the list is very small. This is attributed to the fact that the comparison operation is computationally very cheap.

VI. Related Work

An efficient anonymous batch authentication scheme called ABAH is proposed in [14]. The objective of this scheme is to achieve users' privacy and batch authentication of messages. The RSU is responsible for authenticating the vehicles by checking their revocation status when it receives a message from a vehicle. Then, it securely sends a group key to vehicles if authentication succeeds. If the pseudonym is found in the CRL, the RSU does not send the group key to the revoked vehicle. Temporary Anonymous Certified Keys (TACKs) which is a VANET key management scheme is proposed in [15]. The traffic regions are divided and assigned to registration authorities. The registration authority act as a certificate authority that issue short-lived certificates to the vehicle when they enter its boundaries after authenticating them. Vehicles use group signature [9] to authenticate their messages sent to the RAs. The vehicles use the short-term certificates in a limited geographic area which provides short-term linkability. Then, they should update these short-term certificates when they move to a new RA boundary.

In order to allow timely-manner distribution of large CRLs in VANETs, [16] proposes to partition the CRLs into smaller pieces based on geographic distribution of vehicles. Each RSU receives a piece of the CRL from the certificate authority and shares it with the vehicles in its vicinity. Local Eviction of Attackers by Voting Evaluators (LEAVE) scheme is proposed in [5] which is based on voting to revoke a misbehaved vehicle. The vehicles broadcast messages to warn surrounding vehicles if it detects a malicious neighbor. When a vehicle receives warning message, it adds the vehicle to an accusation list. This is considered as an intermediate stage before deciding to report the vehicle to the CA. Once a vehicle receives a certain number *a predefined threshold* of warning messages against a certain vehicle, it adds it to a black list and reports the accused vehicle to the nearest CA to perform the revocation.

VII. Conclusion

Revocation of the credentials of an attacker who possesses a large number of pseudonyms is a challenging problem. In this paper, we have proposed a scalable revocation scheme that allows the revocation of a large number of pseudonyms by publishing a fixed-sized trapdoor. This is more efficient than adding a large number of pseudonyms to the certificate revocation list in terms of revocation storage and computation overhead. We used chameleon hashing construct in the process of generating pseudonyms and linking them in case of misbehaviour. The published trap door allows a verifier to link the pseudonyms of attackers. By deliberately linking the pseudonyms, an attacker can be easily tracked and its identity can be revealed. Since, it is important for the revocation authority to validate the revocation requests to avoid revoking the credentials of a legitimate vehicle, a voting scheme based on multi-signature has been proposed to increase the creditability of revocation requests. The proposed scheme is evaluated and the results indicated that it is more efficient in terms of communication and computation overhead than conventional CRLs to publish revocation information.

References

[1] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Computer Communications*, vol. 63, pp. 11–23, 2015.

[2] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," *The Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 11–21, 2005.

[3] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," *The Proc. of the IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks*, pp. 1–6, 2013.

[4] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on hmac for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[5] 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, Oct 2007.

[6] H. A. Falasi and E. Barka, "Revocation in VANETs: A survey," *The Proc. of the 2011 International Conference on Innovations in Information Technology*, pp. 214–219, April 2011.

[7] P. Vijayakumar, M. Azees, and L. J. Deborah, "Cpav: Computationally efficient privacy preserving anonymous authentication scheme for Vehicular Ad Hoc Networks," *The Proc. of the 2nd IEEE International Conference on Cyber Security and Cloud Computing*, pp. 62–67, Nov 2015.

[8] 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," *The Proc. of the IEEE SoutheastCon 2010 (SoutheastCon)*, pp. 380–383, March 2010.

[9] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," *The Proc. of the 11th ACM conference on Computer and communications security*, pp. 168–177, 2004.

[10] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[11] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[12] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," *International Workshop on Public Key Cryptography*, pp. 257–273, 2006.

[13] Miracl, "Multiprecision integer and rational arithmetic c/c++ library."

[14] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on hmac for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, Aug 2016.

[15] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," *The Proc. of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON*, pp. 1–9, 2009.

[16] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," *The Proc. of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, pp. 86–87, 2008.