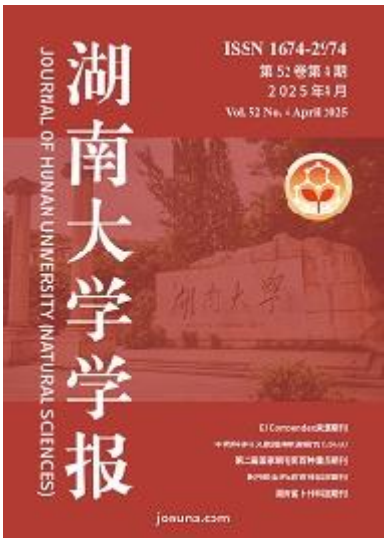

Journal of Hunan University

(Natural Sciences)

Vol. 52 No. 4

April 2025

Available online at

https://jonuns.com

Open Access Article

https://doi.org/10.55463/issn.1674-2974.52.4.6

Efficient Revocation of Malicious Vehicles in VANETs

Mahtab[1], Qazi Ejaz Ali[1*], Farkhund Iqbal[2], Waheed Ur Rehman[1], Abdul Haseeb Malik[1], Tabinda Salam[3]

[1] Department of Computer Science, University of Peshawar, Pakistan

[2] College of Technological Innovation, Zayed University, Abu Dhabi, United Arab Emirates

[3] Department of Computer Science, Shaheed Benazir Bhutto Women University Peshawar, Pakistan

* Corresponding author: qaziejazali@uop.edu.pk

Article History:

Received: March 16, 2025
Revised: April 17, 2025
Revised: April 29, 2025
Accepted: May 4, 2025
Published: May 30, 2025

Abstract: Intelligent Transport Systems (ITS) leverage cutting edge technology to enhance the reliability, protection and effectiveness of transportation. Dedicated Short Range Communication (DSRC) is the mean by which Vehicular Ad Hoc Networks (VANETs) provide connectivity among vehicles in form of vehicles to vehicle (V2V) and vehicle to roadside infrastructure (V2I). Maintaining safe connections in VANETs is a major issue due to malicious behavior of unlawful vehicles. Therefore, in order to protect VANETs, malicious vehicles should be revoked, for this purpose Certificate Revocation List (CRL) is distributed by the authorities among the VANETs users. However, due to the passage of time CRL size increased and becomes large, which produces delays in checking and verification of messages and results in disruption. Therefore, dissemination, updating, and searchable processes of traditional CRL techniques face latency and scalability problems. This paper aims to overcome these challenges by eliminating dependency on

CRLs, introducing efficient revocation verification, and enabling a self-sufficient revocation mechanism. A novel ERMV approach is proposed, in which Bad-Hash is applied only to pseudonym certificates of revoked vehicles, which facilitates onboard, independent certificate status verification without the need to distribute, obtain or check CRLs. The proposed technique ensures rapid certificate status verification with minimal computational and communication overheads. The results show that the proposed technique can verify over 900 messages in a 300millisecond time frame, which illustrates that the proposed technique can work efficiently in sparse and dense scenarios with less computational and communication overheads.

Keywords: Vehicular Ad Hoc Networks (VANETs); authentication; revocation; hash.

有效撤销车联网中的恶意车辆

摘要：智能交通系统 (ITS) 利用尖端技术来提升交通运输的可靠性、安全性和效率。专用短程通信 (DSRC) 是车载自组织网络 (VANET) 的一种方式，它通过车对车 (V2V) 和车对路边基础设施 (V2I) 两种方式为车辆提供连接。由于非法车辆的恶意行为，维护 VANET 中的安全连接是一个重大问题。因此，为了保护 VANET，应该吊销恶意车辆的证书吊销列表 (CRL)，为此，主管部门会在 VANET 用户之间分发证书吊销列表 (CRL)。然而，随着时间的推移，CRL 的大小不断增加，导致消息检查和验证延迟，并最终导致中断。因此，传统 CRL 技术的传播、更新和可搜索过程面临延迟和可扩展性问题。本文旨在通过消除对 CRL 的依赖、引入高效的吊销验证机制以及实现自给自足的吊销机制来克服这些挑战。提出了一种新颖的 ERMV 方法，该方法仅对已撤销车辆的假名证书应用 Bad-Hash，从而方便在车上进行独立的证书状态验证，无需分发、获取或检查 CRL。该技术能够以最小的计算和通信开销快速验证证书状态。结果表明，该技术能够在 300 毫秒的时间内验证超过 900 条消息，这表明该技术能够在稀疏和密集场景下高效工作，并且计算和通信开销更低

关键词：车载自组织网络（VANET）；认证；撤销；哈希

1. Introduction

Intelligent Transport System (ITS) encourages the sustainability, effectiveness, and optimize transportation systems and services by utilizing cutting edge technology, communication tools, including information management strategies., thereby improving public safety, travel comfort, and reducing travel costs [1].

A key component of ITS is the Vehicular Ad Hoc Networks (VANETs), which enables vehicles to communicate with each other in the form of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). VANETs utilize Dedicated Short-Range Communication (DSRC), also known as IEEE 802.11P to deliver consistent, minimal latency transfers of information at data speeds of up to 27 Mbps across a range of 100 to 1,000 meters [2].

The primary components of VANETs include Trusted Authorities (TAs), Road Side Unit (RSU), and On-Board Unit (OBU). TAs manage network operations and ensure system integrity, RSUs installed along roadways enable communication between vehicles OBU and TAs, OBUs are installed within vehicles that enable the vehicles to exchange information such as road conditions and traffic updates [3-4].

The wireless characteristics of VANETs expose it to various security threats, such as Denial of service (DoS), Sybil, spoofing, and sinkhole attacks [2,5]. To mitigate these threats, robust authentication mechanisms are essential. Public Key Infrastructure (PKI) is commonly used to secure VANETs using X.509 standard for the generation, distribution, and revocation of digital certificates [6]. Vehicles typically use short-term pseudonym certificates for authentication and privacy, with the need for frequent renewals around 25,000 times within a five-year duration [7]. The systematically revocation of certificates is essential to maintain network integrity by invalidating certificates that are involved in malicious activities or no longer valid.

Revocation is the procedure of making valid certificates that have already been granted revoke in order to remove malicious and unauthorized vehicles

from accessing the network. In active revocation, this process is documented in the Certificate Revocation List (CRL) should be managed efficiently, to distribute and use the information to ensure all vehicles received the information regarding revoked vehicles. Effective distribution of CRL is vital for VANETs security. Various methods have been proposed to enhance CRL distribution and checking. However, the CRL based schemes has communication delays that provide opportunity for the attacks.

In [8], the researchers proposed a technique to enhance scalability and reduce distribution delays by dividing the original CRL into smaller segments, thereby improving the distribution of an individual CRL. However, this method does not optimize memory usage and computational resources. Similarly, broadcasting the CRL was proposed [9], but this approach overlooks the impact of distributing large CRLs across wide areas with a large number of vehicles. Hierarchical CRL distribution, dividing CRLs into global and regional types, addresses scalability and size issues but adds infrastructure complexity [10]. Merkle hash trees facilitate efficient revocation checking by distributing the root hash value to vehicles, although challenges with increasing numbers of revoked certificates persist [11]. A technique was designed [12] based on Bloom filters probability data structure that compress CRLs to reduce bandwidth requirements for distribution. However, the suggested approach is producing negative results, which leads to show legitimate vehicle as malicious.

A dual Bloom filter was proposed [10] to reduce the rate of false positives, area and trip-specific CRLs reduced overheads by providing vehicles with CRLs relevant only to their operational areas and trip durations [13]. Although this method shortens distribution delays, the CRL is still required, its dissemination and checking are still necessary for system security. Fog computing combined with Merkle hash trees aims to replace time-consuming CRL checking with more efficient methods, though these approaches introduced new complexities and costs by implementing fog nodes [14]. The scheme outlined in [15] employs RSUs to generate the updated secrets, necessary for vehicles to create their secret keys. If a malicious vehicle is identified, the RSU will cease generating secrets for that specific vehicle. However, since RSUs are positioned in open areas, they are vulnerable to DoS attack. Decentralized voting-based techniques for revocation still require CRL distribution and verification [16]. In [17], the authors suggested utilizing an activation-code-based approach in place of CRL, wherein a certificate is utilized upon receiving its activation code. However, the activation code dissemination is challenging because of ineffective network and computational overheads.

The above-mentioned schemes, in which there is a need for distribution, downloading and checking the CRL to recognize and block revoked vehicles, which introduces considerable overheads. It is not a desirable approach in the VANETs. Therefore, it is important to eliminate malicious vehicles as soon as realistic to revoke them from doing more malicious activities.

The purpose of this paper is to devise a revocation scheme that will enable vehicles to identify a revoked vehicle in V2V communication despite the need for an updated CRL distribution, in order to guarantee the objectives listed below:

.

- To efficiently identify a revoked vehicle
- To reduce message authentication time
- To provide a secure communication

The remaining parts of the paper are organized as follows: Section 2 reviews the relevant literature, Section 3 discusses the network model, Section 4 demonstrates results and discussion, Section 5 presents conclusion.

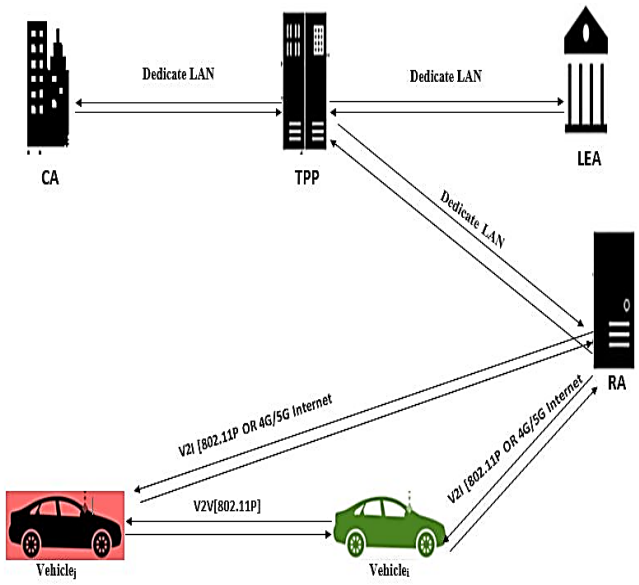

Figure 1. System Model (developed by the authors)

2. Literature Review

Management and revocation of credentials are essential components in the protection of V2V and V2I, which is called vehicle to everything (V2X) communication. The Security Credential Management System (SCMS) is used in the US, whereas the European Telecommunications Standards Institute (ETSI) provides a structure for V2X credential management in Europe [18-19]. Both of them utilized long term credentials for authentication and secure communication in V2X interactions. Long-term credentials are embedded in vehicles at manufacture in the form of private keys or as certificates issued upon enrollment in the ITS infrastructure, while pseudonym, which are short lived with lifespans of up to several weeks are changed periodically to prevent tracking and enhance privacy [20-21].

Compromised vehicles with valid credentials pose significant risks by disseminating malicious data that can lead collisions risks. Similar attack scenarios have been investigated by Sun et al. [22] and referenced in [23]. Once detected, a rapid certificate revocation process must be initiated to prevent further damage. Designing an efficient certificate revocation mechanism for vehicular networks involves addressing two key requirements, which are timely distribution of revocation information and ensuring that the revocation checking process is efficient enough to meet latency requirements [23].

Active revocation, a widely adopted approach in systems like SCMS, involves invalidating pseudonym certificates through the creation and regular updating of CRLs, which contains entries for revoked pseudonyms through which vehicles decide whether to accept or reject messages from other vehicles. While this method is essential for maintaining security, it presents challenges related to managing the increasing size of the CRL, which can lead to substantial computational and communication overhead, [24-25]. Therefore, CRL based techniques must balance the need for timely revocation information with efficient distribution and verification to avoid latency issues [26].

To improve CRL distribution efficiency, various strategies have been proposed. RSU placement optimization, as demonstrated in [27]. However, due to limit number of RSUs, the accurate information regarding revocation cannot be available sometimes. To address this, it was suggested using mobile nodes like public safety vehicles to assist in CRL dissemination [28]. However, infrastructure is complex and the mobile nature of the nodes can lead to the unavailability of particular nodes during crucial instances. Leveraging cellular networks were explored to extend CRL delivery in areas with limited RSU coverage [29]. At high speeds, vehicles may lose connectivity or encounter areas with poor network coverage, complicating their ability to access the latest CRL.

Additional techniques like Bloom filters, aiming to optimize bandwidth usage and improve distribution efficiency [12] proposed, however it can encounter false positive. Geographical distribution segments the network into smaller regions to manage CRL size and enhance delivery [10, 13]. Its infrastructure is complex and when vehicle enters new zone without timely access to that particular zone CRLs, it can mislead in identifying revoked vehicles.

As it also important to efficiently use revocation information after receiving or getting it. Bloom filters offer faster verification of CRL but introduces false positives [30]. Merkle Hash Trees represent a more advanced technique for CRL management, offering reduced storage requirements and faster verification. A trapdoor-based technique was introduced [31] to further minimize delays in pseudonym-based networks. Although these methods minimize storage requirements and verification delays, they still necessitate the distribution and verification of revocation information during V2V communication. Furthermore, edge computing paradigms, as explored in [32-33], have shown promise in reducing revocation costs and facilitating efficient CRL management. However, edge-based approaches also introducing delays [19]. Despite ongoing advancements, recent surveys [34, 24] indicate that many of the proposed solutions for credential revocation in V2X systems still face significant challenges in terms of efficiency, scalability, and real-time performance.

Similarly, passive revocation uses short lived pseudonyms, reducing the need for traditional revocation methods. However, it may allow malicious vehicles to operate until pseudonyms expire, posing potential risks [35-36]. The Online Certificate Status Protocol (OCSP) gives revoked status updates but suffers from latency, limited infrastructure availability, and scalability issues [37]. Tesei et al. [23] proposed a Distributed Ledger Technology (DLT) based revocation approach to address scalability and delays in revocation checking. However, in high-speed scenarios the intermitted connectivity problem affects the verification process.

The Activation Code for Pseudonym Certificates (ACPC) method, which employs activation code to manage multiple pseudonym certificates, reduces certificate size but can increase bandwidth usage and latency due to the overhead of broadcasting activation codes [38]. Decentralized self-revocation systems enable vehicles to manage their own credentials [21, 39], but these decentralized techniques using self-revocation to remove its certificates and prone to Sybil attacks

Therefore, here is a necessity for a scheme that enables vehicles to identify a revoked vehicle in V2V communication without relying on the distribution of activation codes, online checks, or CRLs. Such an approach can reduce message verification requirements, minimize the vulnerability window, and improve security.

3. Network Model

This section includes the System model, Design Goal, and Methodology of the proposed research work.

3.1 System Model

The system model consists of the following entities.

Malicious Vehicle (Vj)

If a vehicle, designated as V_j, disseminates misleading information, obstructs communication, or breaches rules, it is deemed malicious.

Legitimate Vehicle (Vi)

V_i is designated as a valid and legal vehicle. When V_i finds unlawful conduct, it reports to the Revocation Authority (RA). V_i's timely reporting helps maintain network security by isolating malicious vehicles.

Revocation Authority (RA)

It is an authoritative source responsible for revoking malicious vehicles. Upon receiving a report, the RA initiates revocation by informing TPP about malicious vehicle, calculating and broadcasting Bad-Hash for that malicious vehicle. The RA ensures network trust by managing revocations effectively.

Temporary Pseudonym Provider (TPP)

The TPP is a very trustworthy source that governs the distribution of certificates to vehicles. It carries out two crucial tasks that are given and update certificates to secure communication and managing Blacklist called Blocked Registration Certificate List (BRCL) to guarantee that revoked vehicles are unable to regain or update the pseudonym certificate to access the VANETs.

Certificate Authority (CA)

CA is a trustworthy source that issues Registration Certificates (RCs), which are necessary for vehicles to obtain Temporary Pseudonym Certificates (TPCs). A valid RC is required for a vehicle to TPC to communicate securely in the network.

Law Enforcement Authority (LEA)

The government authority in charge of maintaining norms within the VANETs. Once a vehicle is recognized as harmful and revoked by the RA, the LEA is alerted to pursue legal or administrative procedures according to the laws.

3.2 System initialization

When a vehicle wants to be part of VANETs, in the proposed technique of efficient revocation of malicious vehicles (ERMV), vehicles should have Temporary Pseudonym Certificates (TPC) to provide security in network. When vehicle first enter in the network having Initial Registration Code (IRC) which is given to each vehicle once through system. The vehicle sends the IRC to certificate authority to get Registration Certificate (RC), the CA checks whether the vehicle, that want to get RC is revoked or not by checking its IRC in its database, if found it means it is already registered revoked vehicle, and will not issue RC, if not found, then it issues an RC to the vehicles. After getting the RC vehicle can get TPC from TPP by providing its RC, TPP will check its BRCL against the vehicle RC, if its RC is listed in BRCL, it means it is a revoked vehicle, if not in BRCL vehicle will get TPC which is necessary to participate and communicate in the network. In this framework the identity of vehicle is not vulnerable because the vehicles get its pseudonyms certificate in distributed manner and if one entity in network is compromised, still vehicle real identity cannot be revealed.

3.3. Design Goals

The following are the design goals of the proposed technique.

1. **Enhanced Scalability through CRL Elimination**: The elimination of the CRL improves the system's scalability by removing the need for vehicles to check a centralized repository for revoked certificates, thereby reducing computational and communication overheads.
2. **Efficient Revocation Verification:** The revocation process is made efficient by enabling vehicles to rapidly verify certificate statuses without scanning long lists.
3. **Self-Sufficient Revocation Mechanism:** The system eliminates the need for external entities that enables vehicles to independently verify revocation status through onboard algorithms, therefore simplifying the overall revocation process.

3.4. Methodology

The proposed technique of ERMV as illustrated in Figure 2, which demonstrates that how adversely vehicles are revoked.

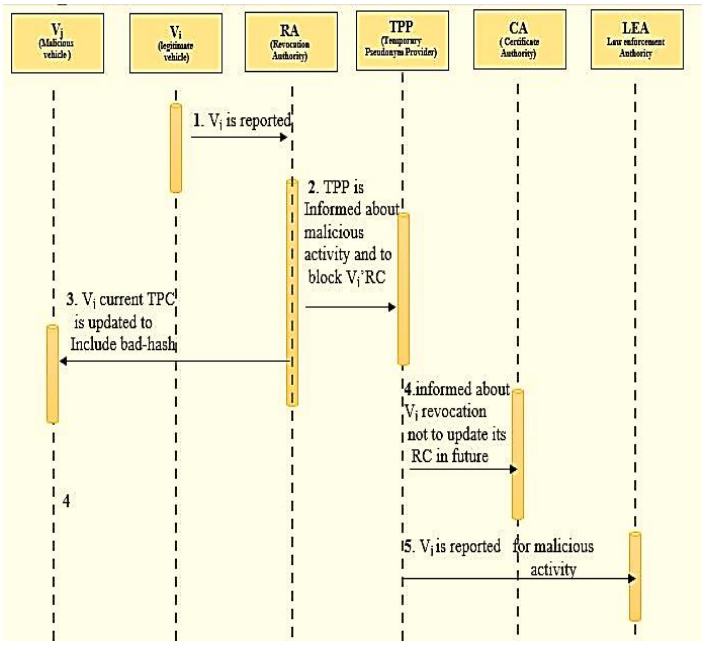

Figure 2. Proposed Methodology (developed by the authors)

The OBU algorithm shown in Figure 3 is designed to identify revoked vehicle during communication between vehicles. The proposed technique of ERMV includes the following steps:

Step 1: The malicious vehicle "V_j" is reported for its unlawful acts to the RA by authentic vehicle "V_i".

Step 2: In order to stop further updates of V_j certificate (TPC), RA notifying the Temporary Pseudonym Provider (TPP) of the adverse action of V_j to add its RC to the BRCL.
Step 3: Computing the Bad-Hash, RA broadcasts the computed Bad-Hash for the revocation, V_j trusted component updates the TPC by adding the Bad-Hash. As result of the Bad-Hash, Vehicles will not verify messages from V_j by utilizing the OBU algorithm.
Step 4: TPP will report unlawful conduct and revocation of V_j to the CA.
Step 5: Regarding adverse conduct of V_j, TPP informs the LEA for legal actions.

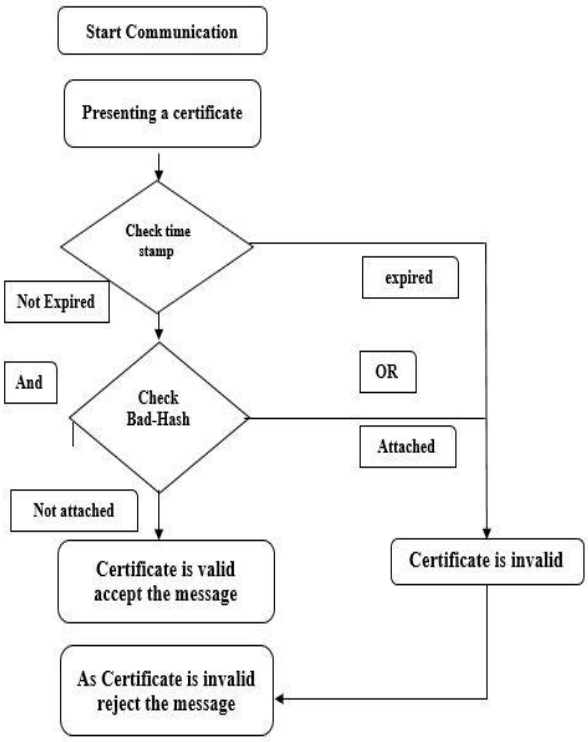

Figure 3. OBU algorithm (developed by the authors)

3.3.1 Proposed Technique (ERMV)

As in the system initialization section 3.2 it is discussed that a vehicle can get its TPC to participate in network. After joining the network if a vehicle (referred to as V_j) tries to interact with another vehicle (referred to as V_i) through V2V interactions. If V_j engages in unlawful behavior, such as sending deceptive or false information, V_i compiles a report and submits it to the RA. This report includes the message (M) V_j attempted to send, within the time of report (R_T) indicating when the report received, and V_j TPC, which serves as a temporary identity the VANET. The report is structured as:

Reporting Message = [M_{Vj} || R_T|| Vj_{TPC}]

The RA starts a series of steps to deal with the adverse vehicle immediately as it gets the complaint. In order to effectively stop V_j from getting new pseudonyms, the RA first informs the TPP to add V_j Registration Certificate (RC) to the BRCL and barring it from future network participation.

To further secure the network and to revoke V_j, the RA generates a "Bad-Hash" using the MD5 hashing algorithm [40], based on V_j certificate serial number. For instance, if the serial number of V_j certificate is 4097 (0x1001), applying MD5 hashing to the string "4097(0x1001)" generates a 128-bit hash value. For example, for this hash output is: d830ff5f3c19cbd12b00f9a5f2f45208.

These Bad-hashes are used to uniquely identify the revoked certificate across the network, ensuring the integrity of the revocation process.

The RA then constructs an Order of Update (OU) message as order of self-revocation (OSR) in [41]. This message includes the malicious message (M), the time of report (T_R), V_j TPC with its public key and other cryptographic details, and the newly generated Bad-Hash, which serves as an indicator of revocation. In order to guarantee that all surrounding vehicles get the revocation information, the OU message is sent to the region where V_j's adverse behavior detected. The information will be transmitted again over a larger region if V_j is not earliest identified as discussed in [41] Upon receiving the OU request message, vehicles in the broadcast area perform a check by comparing the bad-hash in OU with their stored certificates hashes. The structure of OU request,

$$OU\text{-}REQ = M \| T_R \| V_{jTPC} \| \text{ calculated Bad-Hash}$$

where M= message, T_R= time of report, Vj_{TPC}= TPC of malicious vehicle j and *calculated bad-hash* is the hash produced by RA from malicious vehicle serial number.

The Trusted Component (TC) of the vehicle compares the bad-hash included in the OU message with those in the Pseudonym Hash List (PHL). Table 1 shows PHL. The message is accepted only if the bad hash matches an entry in the PHL. In the case that matching occurs, the vehicle certificate is chosen to revoke, and the certificate is modified to reflect this change.

Table 1. Pseudonym Hash List (developed by the authors)

Index	TPC Hashes
1	d830ff5f3c19cbd12b00f9a5f2f45208
2	3c3dbb101f022b7f6e50a35c6a3f2b80
3	b9c8d9a66b1b94b849cd7f536d4c4028
4	912ec803b2ce49e4a541068d4958f317
5	16b4d3248d3e4b9b5a97f7e1e965b4b1
6	e4e86e7c65bfc9c9b77cbf8318b68ae8
7	f6b1b8cbb3bc69c97f1a2d39e6f5c809
8	d1a3a3b2f7ef3e4b8535c4b5a4a0a8d2
9	1c3027be3c5b4987a19b9e8e5e2b8c4e
10	3b5b6e9bdb4a3a0b8e8b7b5a4e6d7c8f

Following a revocation, certificate for the vehicle gets modified by adding the Bad-Hash.

Bad hashes can be included into the pseudonyms as extra fields or key pairs [41-42]. After the revocation, the vehicle sends a confirmation message (OU-CONF) to the RA to verify the completion of the revocation process. The process is shown in Figure 4.

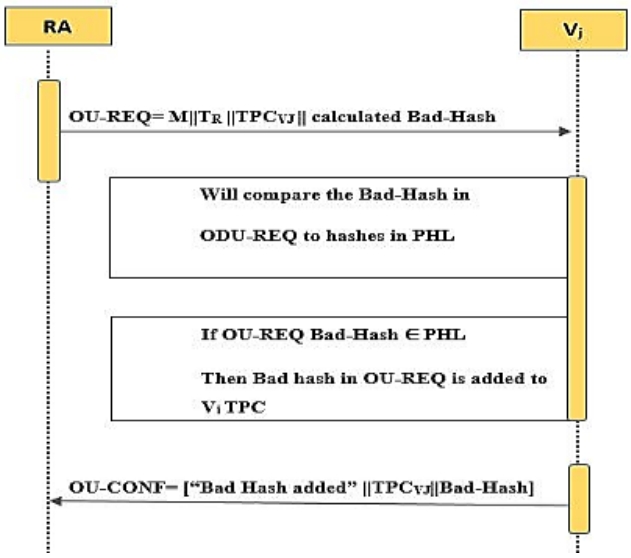

Figure 4. Order of update message (developed by the authors)

Bad-Hashes are added only to revoked vehicle certificates, reducing computational overheads in V2V communication, as they aren't applied to all participant pseudonym certificates.

The Pseudonym Hash List (PHL) optimizes the process by storing MD5-hashed serial numbers of pseudonym certificates. Upon receiving the OU message, vehicles compare the bad-hash with the entries in their PHL. If no match is found, the message is discarded; if a match occurs, the vehicle pseudonym is updated with the Bad- Hash, marking it as revoked. As in previous methods, such as O-tokens and R-tokens [41], [42] part of literature which required embedding additional values into each pseudonym certificate. Unlike these methods, in the ERMV technique not embedding additional values into every certificate for all participant and bad-hash is added only to revoked vehicles certificate, simplifying the process and reducing both storage and computational complexities.

PHL is used to ensure the revocation. During revocation process even if a vehicle alters or deletes its current pseudonym certificate on which the report is submitted to RA for revocation, it cannot bypass the system because the PHL already contains hashes of its current and previous pseudonyms. As well as V_j RC has been added in the BRCL, it cannot update its certificate even if it does not get the OU message right away. A blocked RC causes a swift rejection of requests for certificate renewal because the TPP demands a valid RC for them, making it not possible for V_j to regain access to the network using a different identity.

After V_j pseudonym is revoked, the TPP informs the CA, it prevents V_j from obtaining fresh Registration Certificates (RCs) by blocking its registration code. This action permanently bars V_j from obtaining TPCs and hence cannot be part of VANETs. Furthermore, the TPP informs the LEA of V_j revocation and adverse conduct.

This process ensures the swift and secure revocation of malicious vehicles, maintaining the integrity of the VANETs through strong cryptographic measures, efficient pseudonym management, and collaboration with the relevant authorities to prevent any future threats.

ERMV protocol process is show in algorithm 1.

Algorithm 1 ERMV

1. **Vi → RA**: `Report_Malicious_Activity(Vj)`
2. **RA → TPP**: `Inform_Malicious_Activity(Vj)`
   - **TPP → BRCL**: `Add_RC_to_BRCL(Vj_RC)`
   - **TPP**: `Prevent_TPC_Update(Vj)`
3. **RA → Vj**: `Revoke_Vehicle(Calculate_Bad-Hashes)`
   - **RA → Broadcast**: `Broadcast_Bad-Hashes (Vj)`
   - **Vj_TC**: `Update_TPC_with_Bad-Hashes (Vj_TPC)`
4. **TPP → CA**: `Inform_CA_of_Revocation(Vj)`
5. **CA:** `Do_Not_Update_RC(Vj)`
6. **TPP → LEA:** `Inform_LEA_of_Malicious_Activity(Vj)`

Verifying the authenticity of vehicles during V2V communications is essential for maintaining the security in VANETs. The OBU algorithm, shown in Figure 3, is designed to verify the authenticity of a vehicle TPC. When Vehicle V_j sends a message to Vehicle V_i, it includes its TPC, which V_i must validate. The OBU algorithm is shown in algorithm 2 of two checks, which is listed below.

The receiving vehicle Vi verifies the certificate validity by comparing the current time Now_T with the certificate issuance time TPC_T, and validity period as VP_T.

If $Now_T - TPC_T > VP_T$, the pseudonym is expired, and the message gets eliminated.

If $Now_T - TPC_T \leq VP_T$, since the certificate is legitimate the procedure advances to another phase.

Similarly, algorithm verifies whether pseudonym has a Bad-Hash to check authenticity of the vehicle.

If the Bad-Hash present, the message is denied and the vehicle is recognized as revoked vehicle.

If no Bad-Hash present, the communication is accepting as the pseudonym certificate is valid.

The purpose of the OBU algorithm is to check certificate validity and bad-hash in certificate during V2V communication.

Algorithm 2 (OBU algorithm) Pseudo code

1. $\mathbf{V_j} \rightarrow \mathbf{V_i}$: $M \| V_{jTPC}$
2. $\mathbf{V_i}$: Check TPC_T

- if $Now_T - TPC_T > Validity\text{-}Period_T$, the communication is rejected since the certificate is out of date
- . If $TPC_T \geq (Now_T - Validity\text{-}Period_T)$. Go to the next stage as the certificate is not out of date

3. $\mathbf{V_i}$: Check for Bad-Hashes

- If V_{jTPC} ‖Bad-Hashes. Not to accept the communication.
- If V_{jTPC}||no bad-hashes. Accept the communication.

4. $\mathbf{V_i}$: Approve message M from V_j.

4. Results and Discussion

The proposed ERMV technique is implemented in python [23]. The system used for the implementation is Intel Core i5 CPU with 8GB RAM. Pseudonym certificate template [43], and the CRL files CRL-20000, CRL-30000, and CRL-50000 containing 20,000, 30,000, and 50,000 CRLs records, respectively are among the datasets utilized for the evaluation. The evaluation performance is conducted under three traffic scenarios that are sparse (25 nearby vehicles), medium (50 nearby vehicles), and dense (100 nearby vehicles). According to the DSRC standard, vehicles are required to send messages every 300 milliseconds [44]. Under these scenarios, a vehicle will receive 25, 50 and 100 messages from surrounding vehicles within 300 milliseconds. The goal is to determine the message verification times during V2V communication to safeguard legitimate vehicles from malicious vehicles by checking vehicle certificate status through OBU algorithm.

The script is executed 30 times for each CRL file and 100 times for the ERMV technique. The average execution time is computed to accurately analyze the proposed technique results. The results are shown on the basis of average execution time.

4.1 Computational Complexity of Revocation Status Checking

To examine the computational complexity of the process used to verify and check the status of certificate to ensure it is revoked or not. This complexity is measured by the number of comparison operations needed to check whether a certificate has been revoked. The computational complexity of revocation status checking varies between methods. The traditional method involves verifying a certificate by comparing it with every entry in the CRL. If there are E CRL entries and C certificates, this method has a complexity of O(E)(C) due to E comparisons required for each certificate. In contrast, the ERMV simplifies the process by requiring only one comparison per certificate, irrespective of the number of CRL entries. Consequently, the complexity of this method is O(C), representing a significant reduction in computational effort compared to the traditional approach.

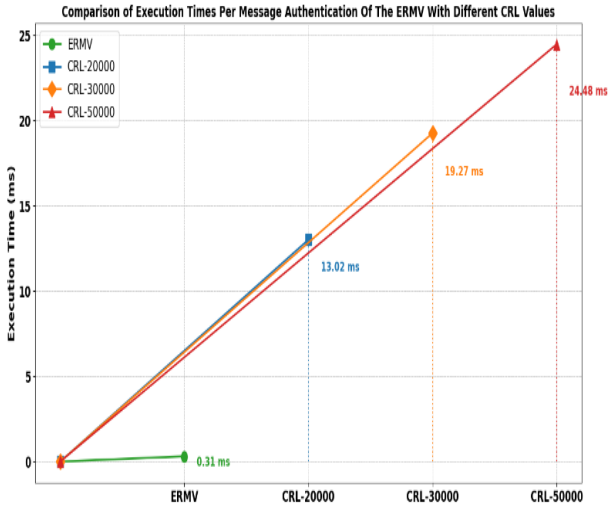

Figure 5. Execution Time per message of the Proposed Technique and CRLs (developed by the authors)

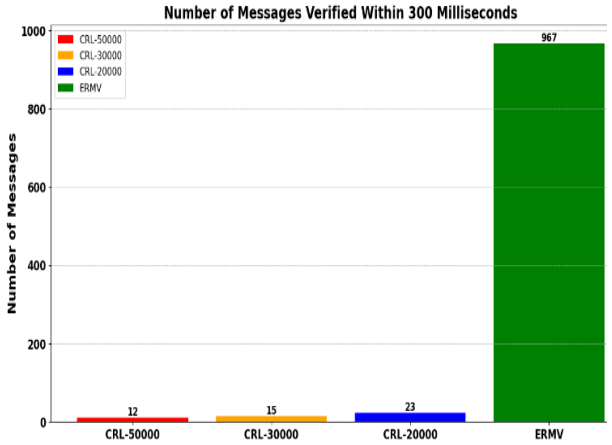

Figure 6. Number of messages verified with 300 milliseconds of the Proposed Technique and CRLs (developed by the authors)

Figure 5 shows the message verification time in the proposed technique compare to CRL, Figure 6 shows verified messages within 300 milliseconds and Figure 7 shows proposed technique performance improvement.

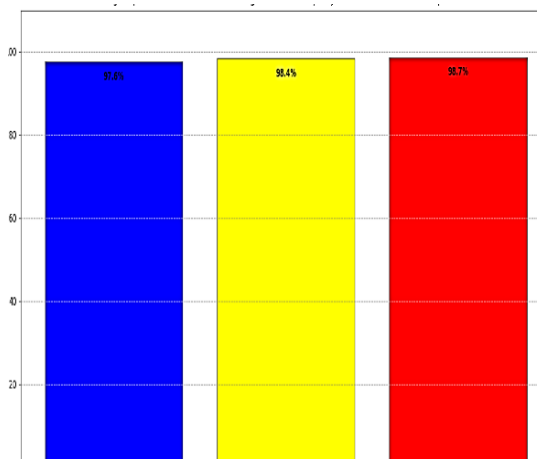

Figure 7. Percentage Improvement of the Proposed technique compared to CRLs (developed by the authors)

4.2 Execution Time Analysis

We compare the execution time required to verify that a vehicle certificate is valid or not using two different search methods, one involving multiple CRLs files and the other using ERMV technique. The traditional method, which involves comparing a vehicle certificate against entries in multiple CRL files, shows a clear increase in execution time with larger CRL files. The average time varies, reflecting the growing computational burden as CRL size increases. In contrast, the ERMV achieves a consistently low execution time, regardless the traffic conditions. The significant reduction in verification time shows the efficiency of the proposed technique. The results are shown in Figures 8, 9, 10 and 11, respectively, which indicates ERMV is better in messages verification than CRLs.

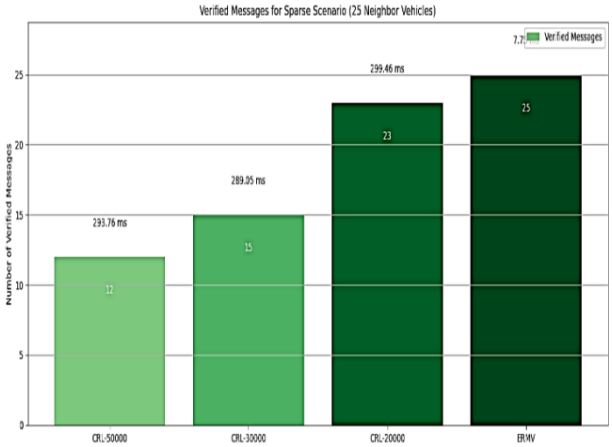

Figure 8. Number of verified messages within 300 milliseconds of the proposed technique compared to CRLs in Sparse scenarios (developed by the authors)

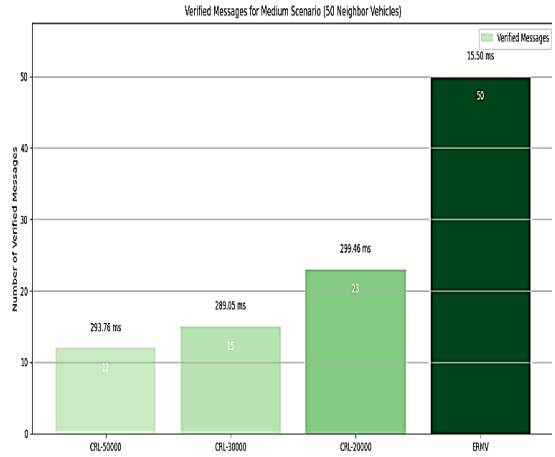

Figure 9. Number of verified messages within 300 milliseconds for proposed technique compared to CRLs in Medium scenarios (developed by the authors)

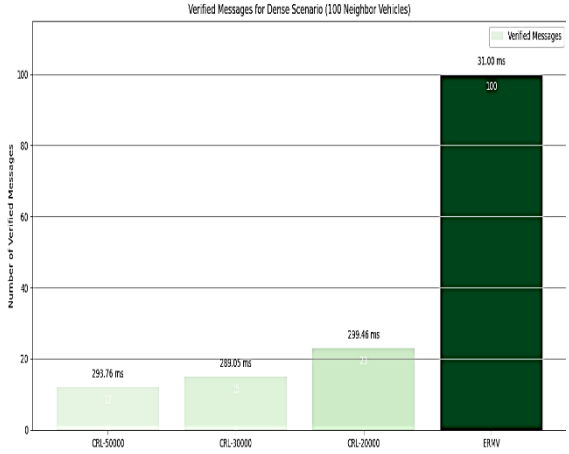

Figure 10: Number of verified messages within 300 milliseconds for proposed technique compared to CRLs in Dense scenarios (developed by the authors)

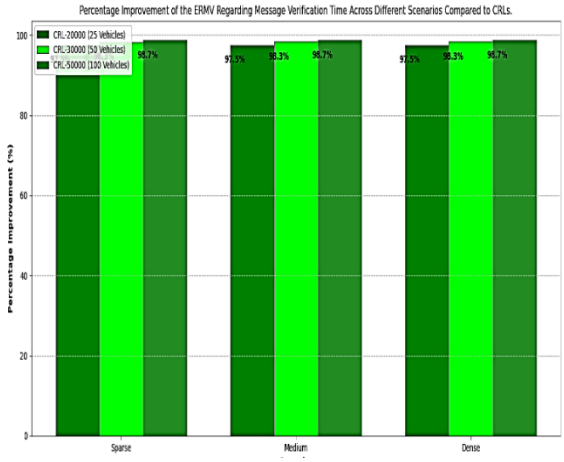

Figure 11: Message verification percentage Improvement of the proposed technique compared to CRLs in Sparse, Medium and Dense scenarios (developed by the authors)

4.3 Message Loss Ratio

The message loss ratio assesses the proportion of messages discarded due to delays in the authentication process, relative to the total number of messages received within different interval in different scenarios. Traditional CRL methods demonstrate increasing message loss ratios as vehicle density and CRL size grow, indicating their limitations in handling higher traffic volumes and extended verification time. In contrast, the proposed technique consistently achieves a zero-message loss ratio across all scenarios, indicating its better performance varying traffic conditions. This makes the proposed technique ERMV highly effective for real-time V2V communication, ensuring reliable message authentication regardless of traffic density. The result is shown in Figures 12, 13, 14 and 15, respectively.

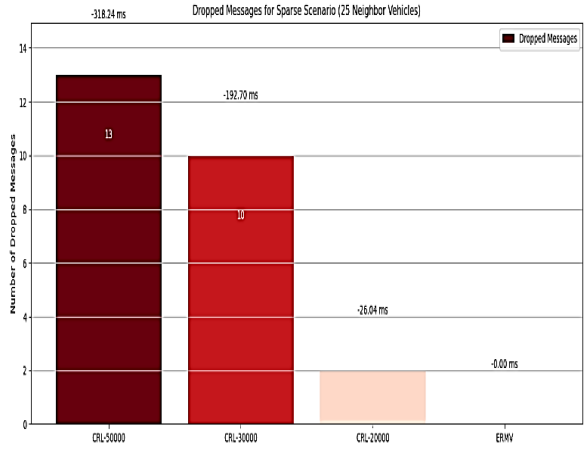

Figure 12: Number of dropped messages within 300 milliseconds of the proposed technique compared to CRLs in sparse scenarios (developed by the authors)

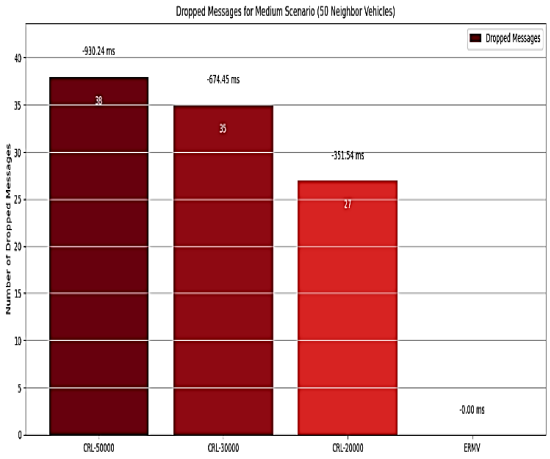

Figure 13: Number of dropped messages within 300 milliseconds of the proposed technique compared to CRLs in Medium scenarios (developed by author)

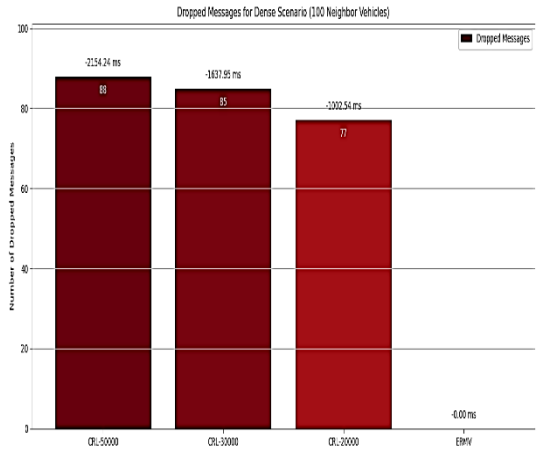

Figure 14. Number of dropped messages within 300 milliseconds of the proposed technique compared to CRLs in Dense scenarios (developed by the authors)

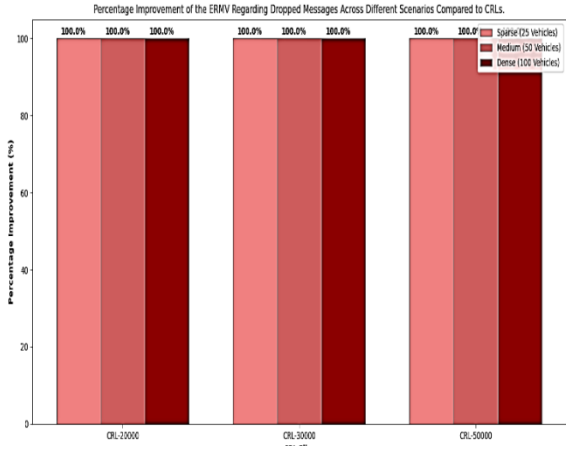

Figure 15: Dropped message percentage Improvement of the proposed technique compared to CRLs in Sparse, Medium and Dense scenarios (developed by the authors)

4.4 End-to-End Delay

In traditional CRL methods, delay rises as the CRL size increase. Due to the increasing time required to verify certificates against larger CRLs and the additional processing burden from more neighboring vehicles in dense scenarios. Specifically, delays grow when CRL entries increases, reflecting the linear relationship between CRL size and processing time. In contrast, the ERMV achieves consistent end-to-end delays, by minimizing the time required for certificate validation, the proposed method ensures that communication remains timely and effective, regardless traffic density. This significant reduction in delay demonstrates the ERMV's performance in maintaining reliable and prompt communication in various traffic conditions.

4.5. Attack Model

In order to realize determined restricted anonymity and concealment, the subsequent diverse kinds of risk

scenarios have been considered in the proposed technique.

1. **Anonymity Protection:** vehicle identities are distributed across multiple entities, so if one entity is compromised, the vehicle identity remains anonymous and secure.
2. **No Self-Creation of Pseudonym Certificates**: In this system, pseudonym certificates are provided through a distributed process, not self-generated by the vehicles. This prevents vehicles from bypassing the revocation process or re-entering the network after being flagged.
3. **Resistance to DoS Attacks:** Once a vehicle is revoked, it can be recognizing by other vehicles even if its network connection is temporarily disrupted, enhancing resilience against traditional Dos and DDoS attacks.
4. **Blocked Pseudonym Updates After Revocation:** Once the RA initiates the revocation process, it instructs the TPP to block the vehicle's RC, preventing any further pseudonym updates.
5. **Guaranteed Revocation through PHL**: Even if a vehicle alters or deletes its pseudonym certificate, revocation is still enforced. The PHL stores the hashes of all previous pseudonyms, ensuring the vehicle is still identified and revoked.

5. Conclusion

In VANETs timely revocation of malicious vehicles are vital to prevent further damages and minimize network disruption. Information about revoked vehicles should be efficiently distributed to legitimate vehicles, in order to decrease the attacking time. This study proposes a novel revocation mechanism for malicious vehicles in VANETs by adding a Bad-Hash into the pseudonym certificates of only the revoked vehicles. The results showed that the proposed technique significantly reduced the time required for vehicle certificate verification compared to traditional CRL based schemes. The ERMV ensures the timely identification of revoked vehicles without the need for CRLs or contacting other entities in the network. Therefore, improving scalability and reducing computational and communication overheads during V2V communication. Similarly, the proposed technique allows for the real time revocation of compromised vehicles without increasing the size of the revoked certificates. As a result, the scheme improves the efficiency of message verification during V2V communication and reduced the attacking time.

5.1. Limitations of the ERMV

In the proposed technique of ERMV, if the attacking vehicle drop OU messages, the revocation will be delayed unless the OU messages are received by the TC of the malicious vehicle.

5.2. Future Research

In future, the proposed technique will be improved to consider Vehicle to Everything (V2X) in fog and cloud environments alongside with more diverse attacks.

Declarations

Author Contributions

All authors contributed to the article structure. All the authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

Funding information is not available.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this manuscript.

References

[1] ALI Q. E., AHMAD N., MALIK A. H., REHMAN W. U., DIN A. U., and ALI G. ASPA: Advanced strong pseudonym-based authentication in intelligent transport system. *PLOS ONE*, 2019, 14(8): e0221213. https://doi.org/10.1371/journal.pone.0221213

[2] ALI Q. E., AHMAD N., MALIK A. H., ALI G., and REHMAN W. U. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. *Applied Sciences*, 2018, 8(10): 1964. https://doi.org/10.3390/app8101964.

[3] AL-SHAREEDA M. A. and MANICKAM S. A systematic literature review on security of vehicular ad-hoc network (VANET) based on VEINS framework. *IEEE Access*, 2023, 11: 46218–46228. https://doi.org/10.1109/ACCESS.2023.3274774.

[4] JAN S. A., AMIN N. U., OTHMAN M., ALI M., UMAR A. I., and BASIR A. A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges, and open issues. *IEEE Access*, 2021, 9: 153701–153726. https://doi.org/10.1109/ACCESS.2021.3125521.

[5] SAMARA G., EID M. B., ALJAIDI M., ALMATARNEH S., RASMI M., ALAZAIDEH R., and AL-LAHHAM Y. Vulnerabilities in Vehicular Ad Hoc Networks and Possible Countermeasures. *Proceedings of the 2022 International Arab Conference on Information Technology (ACIT)*, *IEEE*, 2022, November: 1-5. https://doi.org/10.1109/acit57182.2022.9994082.

[6] KUMAR H., and SINGH D. Smart certificate revocation list exchange in VANET. *Proceedings of the 12th International Conference on Computational Intelligence and Communication Networks* (CICN), IEEE, 2020, September: 210-214. https://doi.org/10.1109/CICN49253.2020.9242643.

[7] HAAS J. J., HU Y. C., and LABERTEAUX K. P. Efficient certificate revocation list organization and distribution. *IEEE Journal on Selected Areas in Communications*, 2011, 29(3): 595–604. https://doi.org/10.1109/jsac.2011.110309.

[8] PAPADIMITRATOS P., MEZZOUR G., and HUBAUX J. P. Certificate revocation list distribution in vehicular communication systems. *Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking*, San Francisco, 2008: 86-87. https://doi.org/10.1145/1410043.1410062.

[9] RABIEH K., MAHMOUD M. M., AKKAYA K., and TONYALI S. Scalable certificate revocation schemes for smart grid AMI networks using Bloom filters. *IEEE Transactions on Dependable and Secure Computing*, 2015, 14(4): 420-432. https://doi.org/10.1109/TDSC.2015.2467385.

[10] TULADHAR K. M., and LIM K. Efficient and scalable certificate revocation list distribution in hierarchical VANETs. *Proceedings of the IEEE International Conference on Electro/Information Technology* (EIT), 2018: 620-625. https://doi.org/10.1109/EIT.2018.8500150.

[11] GAÑÁN, C., MUÑOZ, J. L., ESPARZA, O., MATA-DÍAZ, J., and ALINS, J. EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. *Pervasive and Mobile Computing*, 2015, 21: 75-91. https://doi.org/10.1016/j.pmcj.2014.01.002

[12] RIGAZZI G., TASSI A., PIECHOCKI R. J., TRYFONAS T., and NIX A. Optimized certificate revocation list distribution for secure V2X communications. *Proceedings of the IEEE 86th Vehicular Technology Conference (VTC-Fall)*, IEEE, 2017: 1–7. https://doi.org/10.1109/vtcfall.2017.8288287

[13] KHODAEI M., and PAPADIMITRATOS P. Scalable & resilient vehicle-centric certificate revocation list distribution in vehicular communication systems. *IEEE Transactions on Mobile Computing*, 2021, 20(7): 2473-2489. https://doi.org/10.1109/tmc.2020.2981887.

[14] ALRAWAIS A., ALHOTHAILY A., MEI B., SONG T., and CHENG X. An efficient revocation scheme for vehicular ad-hoc networks. *Procedia Computer Science*, 2018, 129: 312–318. https://doi.org/10.1016/j.procs.2018.03.081

[15] WANG Y., ZHONG H., XU Y., CUI J., and WU G. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs. *IEEE Systems Journal*, 2020, 14(4): 5373–5383. https://doi.org/10.1109/jsyst.2020.2977670.

[16] ASGHAR M., PAN L., and DOSS R. An efficient voting-based decentralized revocation protocol for vehicular ad hoc networks. *Digital Communications and Networks*, 2020, 6(4): 422–432. https://doi.org/10.1016/j.dcan.2020.03.001.

[17] WANTORO J., and MAMBO M. Efficient and privacy-preserving certificate activation for V2X pseudonym certificate revocation. *Journal of Sensor and Actuator Networks*, 2022, 11(3): 51. https://doi.org/10.3390/jsan11030051

[18] ETSI. Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. European Telecommunications Standard Institute (ETSI). *Technical Specification (TS) TS 102 941*, November 2022, version 2.2.1. ETSI TS 102 941 V2.2.1 https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf

[19] BRECHT B., THERRIAULT D., WEIMERSKIRCH A., WHYTE W., KUMAR V., HEHN T., and GOUDY R. A security credential management system for V2X communications. *IEEE Transactions on Intelligent Transportation Systems*, 2018, 19(12): 3850–3871. https://doi.org/10.1109/tits.2018.2797529.

[20] ETSI I. Intelligent transport systems (ITS); security; pre-standardization study on pseudonym change management. *Technical Report ETSI TR 103 415 V1.1*, 2018, April. https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf.

[21] SCOPELLITI G., BAUMANN C., ALDER F., TRUYEN E., and MÜHLBERG J. T. Efficient and timely revocation of V2X credentials. *Proceedings 2024 Network and Distributed System Security Symposium*, 2024: 1-20 https://doi.org/10.14722/ndss.2024.24017.

[22] SUN Z., LIU R., HU H., LIU D., and YAN Z. Cyberattacks on connected automated vehicles: A traffic impact analysis. *IET Intelligent Transport Systems*, 2022, 17(2): 295–311. https://doi.org/10.1049/itr2.12259.

[23] TESEI A., LATTUCA D., LUISE M., PAGANO P., FERREIRA J., and BARTOLOMEU P. C. A transparent distributed ledger-based certificate revocation scheme for VANETs. *Journal of Network and Computer Applications*, 2023, 212: 103569. https://doi.org/10.1016/j.jnca.2022.103569.

[24] YOSHIZAWA T., SINGELÉE D., MUEHLBERG J. T., DELBRUEL S., TAHERKORDI A., HUGHES D., and PRENEEL B. A survey of security and privacy issues in V2X communication systems. *ACM Computing Surveys*, 2023, 55(9): 1–36. https://doi.org/10.1145/3558052.

[25] SIMPLICIO M. A., COMINETTI E. L., KUPWADE PATIL H., RICARDINI J. E., and SILVA M. V. M. ACPC: Efficient revocation of pseudonym certificates using activation codes. *Ad Hoc Networks*, 2019, 90: 101708. https://doi.org/10.1016/j.adhoc.2018.07.007.

[26] GANAN C., MUNOZ J. L., ESPARZA O., MATA-DIAZ J., ALINS J., SILVA-CARDENAS C., and BARTRA-GARDINI G. RAR: Risk aware revocation mechanism for vehicular networks. *Proceedings of the 2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, 2012: 1–5. https://doi.org/10.1109/vetecs.2012.6239941.

[27] KONDAREDDY Y., DI CRESCENZO G., and AGRAWAL P. Analysis of certificate revocation list distribution protocols for vehicular networks. *Proceedings of the 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, 2010: 1–5. https://doi.org/10.1109/glocom.2010.5683985.

[28] CHEN J., CAO X., ZHANG Y., XU W., and SUN Y. Measuring the performance of movement-assisted certificate revocation list distribution in VANET. *Wireless Communications and Mobile Computing*, 2011, 11(7): 888–898. https://doi.org/10.1002/wcm.858.

[29] LEQUERICA I., MARTINEZ J. A., and RUIZ P. M. Efficient certificate revocation in vehicular networks using

NGN capabilities. *Proceedings of the 2010 IEEE 72nd Vehicular Technology Conference - Fall*, 2010: 1–5. https://doi.org/10.1109/vetecf.2010.5594232.
[30] QI J., and GAO T. A privacy-preserving authentication and pseudonym revocation scheme for VANETs. *IEEE Access*, 2020, 8: 177693–177707. https://doi.org/10.1109/access.2020.3027718.
[31] RABIEH K., PAN M., HAN Z., and FORD V. SRPV: A scalable revocation scheme for pseudonyms-based vehicular ad hoc networks. *Proceedings of the 2018 IEEE International Conference on Communications (ICC)*, 2018, 1–6. https://doi.org/10.1109/icc.2018.8422736.
[32] SUN Y., FENG Z., HU Q., and SU J. An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. *Security and Communication Networks*, 2011, 5(1): 79–86. https://doi.org/10.1002/sec.302.
[33] . YANG A., WENG J., YANG K., HUANG C., and SHEN X. Delegating Authentication to Edge: A Decentralized Authentication Architecture for Vehicular Networks. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(2): 1284–1298. https://doi.org/10.1109/tits.2020.3024000.
[34] WANG Q., GAO D., and CHEN D. Certificate Revocation Schemes in Vehicular Networks: A Survey. *IEEE Access*, 2020, 8: 26223–26234. https://doi.org/10.1109/access.2020.2970460.
[35] HICKS C., and GARCIA F. D. A Vehicular DAA Scheme for Unlinkable ECDSA Pseudonyms in V2X. *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2020: 460–473. https://doi.org/10.1109/eurosp48549.2020.00036.
[36] VERHEUL E., HICKS C., and GARCIA F. D. IFAL: Issue First Activate Later Certificates for V2X. *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019: 279–293. https://doi.org/10.1109/eurosp.2019.00029.
[37] SANTESSON S., MYERS M., ANKNEY R., MALPANI A., GALPERIN S., and ADAMS C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. *RFC Editor*, 2013. https://doi.org/10.17487/rfc6960.
[38] SIMPLICIO M. A., COMINETTI E. L., KUPWADE PATIL H., RICARDINI J. E., and SILVA M. V. M. Revocation in Vehicular Public Key Infrastructures: Balancing privacy and efficiency. *Vehicular Communications*, 2021, 28: 100309. https://doi.org/10.1016/j.vehcom.2020.100309.
[39] LARSEN B., GIANNETSOS T., KRONTIRIS I., and GOLDMAN K. Direct anonymous attestation on the road: efficient and privacy-preserving revocation in C-ITS. *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021: 48–59. https://doi.org/10.1145/3448300.3467832.
[40] SANDHU R. VANETs Security Using Cryptography. *International Journal for Research in Applied Science and Engineering Technology*, 2023, 11(6): 1006–1013. https://doi.org/10.22214/ijraset.2023.53739
[41] FÖRSTER D., LÖHR H., ZIBUSCHKA J., and KARGL F. REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks. *Trust and Trustworthy Computing*, 2015: 193–208. https://doi.org/10.1007/978-3-319-22846-4_12.
[42] WHITEFIELD J., CHEN L., KARGL F., PAVERD A., SCHNEIDER S., TREHARNE H., and WESEMEYER S. Formal Analysis of V2X Revocation Protocols. *Security and Trust Management*, 2017: 147–163. https://doi.org/10.1007/978-3-319-68063-7_10.
[43] LINDEMER S. Digital Certificate Revocation for the Internet of Things. 2019. https://www.diva-portal.org/smash/get/diva2:1331631/FULLTEXT01.pdf.
[44]ISLAM, N. Certificate revocation in vehicular Ad Hoc networks: a novel approach. *Proceedings of the International Conference on Networking Systems and Security* (NSysS), 2016: 1–5. https://doi.org/10.1109/nsyss.2016.7400703.

参考文:

[1] ALI Q. E.、AHMAD N.、MALIK A. H.、REHMAN W. U.、DIN A. U. 和 ALI G. ASPA：智能交通系统中基于假名的高级强身份验证。公共图书馆，2019，14(8): e0221213。https://doi.org/10.1371/journal.pone.0221213
[2] ALI Q. E.、AHMAD N.、MALIK A. H.、ALI G. 和 REHMAN W. U. 智能交通系统中的安全和隐私问题、挑战和研究机遇。应用科学，2018，8(10): 1964。https://doi.org/10.3390/app8101964。
[3] AL-SHAREEDA M. A. 和 MANICKAM S. 基于 VEINS 框架的车载自组织网络 (VANET) 安全性系统文献综述。IEEE 访问，2023，11: 46218–46228。https://doi.org/10.1109/ACCESS.2023.3274774。
[4] JAN S. A.、AMIN N. U.、OTHMAN M.、ALI M.、UMAR A. I. 和 BASIR A. 车载自组织网络隐私保护认证方案综述：攻击、挑战和未解决的问题。IEEE 访问，2021，9: 153701–153726。https://doi.org/10.1109/ACCESS.2021.3125521。
[5] SAMARA G.、EID M. B.、ALJAIDI M.、ALMATARNEH S.、RASMI M.、ALAZAIDEH R. 和 AL-LAHHAM Y. 车载自组织网络的漏洞及可能的对策。2022 年阿拉伯国际信息技术会议 (ACIT) 论文集，IEEE，2022 年 11 月：1-5 页。https://doi.org/10.1109/acit57182.2022.9994082。
[6] KUMAR H. 和 SINGH D. 车联网中的智能证书撤销列表交换。第 12 届计算智能与通信网络国际会议 (CICN) 论文集，IEEE，2020 年 9 月：210-214 页。https://doi.org/10.1109/CICN49253.2020.9242643。
[7] HAAS J. J.、HU Y. C. 和 LABERTEAUX K. P. 高效的证书撤销列表组织与分发。《IEEE 通信选定领域期刊》，2011，29(3): 595–604。https://doi.org/10.1109/jsac.2011.110309。
[8] PAPADIMITRATOS P.、MEZZOUR G. 和 HUBAUX J.

P. 车载通信系统中的证书撤销列表分发。第五届 ACM 车辆互联网络国际研讨会论文集，旧金山，2008：86-87。https://doi.org/10.1145/1410043.1410062。

[9] RABIEH K.、MAHMOUD M. M.、AKKAYA K. 和 TONYALI S. 使用布隆过滤器的智能电网 AMI 网络的可扩展证书撤销方案。IEEE 可靠和安全计算学报，2015，14(4): 420-432 。https://doi.org/10.1109/TDSC.2015.2467385。

[10] TULADHAR K. M. 和 LIM K. 分层车联网中高效且可扩展的证书撤销列表分发。IEEE 国际电子/信息技术会议 (EIT) 论文集，2018：620-625 。https://doi.org/10.1109/EIT.2018.8500150。

[11] GAÑÁN, C.、MUÑOZ, J. L.、ESPARZA, O.、MATA-DÍAZ, J. 和 ALINS, J. EPA：一种用于车辆自组织网络的高效隐私感知撤销机制。《普适与移动计算》，2015，21: 75-91 。https://doi.org/10.1016/j.pmcj.2014.01.002

[12] RIGAZZI G.、TASSI A.、PIECHOCKI R. J.、TRYFONAS T. 和 NIX A. 针对安全 V2X 通信的优化证书撤销列表分发。IEEE第86届车辆技术会议（VTC-Fall）论文集，IEEE，2017：1-7 。https://doi.org/10.1109/vtcfall.2017.8288287

[13] KHODAEI M. 和 PAPADIMITRATOS P. 车载通信系统中可扩展且有弹性的以车辆为中心的证书撤销列表分发。IEEE 移动计算学报，2021，20(7): 2473-2489。https://doi.org/10.1109/tmc.2020.2981887。

[14] ALRAWAIS A.、ALHOTHAILY A.、MEI B.、SONG T. 和 CHENG X. 一种高效的车载自组织网络撤销方案。 Procedia 计算机科学，2018，129：312–318。https://doi.org/10.1016/j.procs.2018.03.081

[15] WANG Y., ZHONG H., XU Y., CUI J., 和 WU G.。一种增强安全身份隐私保护认证方案，支持车联网撤销。IEEE 系统杂志，2020，14(4)：5373–5383 。https://doi.org/10.1109/jsyst.2020.2977670。

[16] ASGHAR M，PAN L， 和 DOSS R。一种高效的基于投票的车载自组织网络分散式撤销协议。数字通信与网络，2020，6(4)：422–432 。https://doi.org/10.1016/j.dcan.2020.03.001。

[17] WANTORO J. 和 MAMBO M. 高效且隐私保护的 V2X 假名证书撤销证书激活方法。《传感器与执行器网络杂志》，2022 年，11(3): 51 。https://doi.org/10.3390/jsan11030051

[18] ETSI。智能交通系统 (ITS)；安全；信任与隐私管理。欧洲电信标准协会 (ETSI)。技术规范 (TS) TS 102 941，2022 年 11 月，版本 2.2.1。 ETSI TS 102 941 V2.2.1 https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf

[19] BRECHT B.、THERRIAULT D.、WEIMERSKIRCH A.、WHYTE W.、KUMAR V.、HEHN T. 和 GOUDY R. 一种用于 V2X 通信的安全凭证管理系统。IEEE 智能交通系统学报，2018，19(12): 3850–3871 。https://doi.org/10.1109/tits.2018.2797529。

[20] ETSI I. 智能交通系统（ITS）；安全性；假名变更管理的预标准化研究。技术报告 ETSI TR 103 415 V1.1，2018 年 4 月。https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf。

[21] SCOPELLITI G.、BAUMANN C.、ALDER F.、TRUYEN E. 和 MÜHLBERG J. T. 高效及时地撤销 V2X 凭证。 2024 年网络与分布式系统安全研讨会论文集，2024：1-20 https://doi.org/10.14722/ndss.2024.24017。

[22] SUN Z., LIU R., HU H., LIU D., 和 YAN Z. 针对联网自动驾驶汽车的网络攻击：交通影响分析。IET 智能交通系统，2022, 17(2): 295–311 。https://doi.org/10.1049/itr2.12259。

[23] TESEI A., LATTUCA D., LUISE M., PAGANO P., FERREIRA J., 和 BARTOLOMEU PC. 一种基于透明分布式账本的车联网证书撤销方案。网络与计算机应用杂志，2023，212: 103569 。https://doi.org/10.1016/j.jnca.2022.103569。

[24] YOSHIZAWA T.、SINGELÉE D.、MUEHLBERG J. T.、DELBRUEL S.、TAHERKORDI A.、HUGHES D. 和 PRENEEL B. V2X 通信系统中的安全和隐私问题调查。ACM 计算调查，2023，55(9): 1–36 。https://doi.org/10.1145/3558052。

[25] SIMPLICIO M. A.、COMINETTI E. L.、KUPWADE PATIL H.、RICARDINI J. E. 和 SILVA M. V. M. ACPC：使用激活码高效撤销假名证书。《自组织网络》，2019，90: 101708。https://doi.org/10.1016/j.adhoc.2018.07.007。

[26] GANAN C.、MUNOZ J. L.、ESPARZA O.、MATA-DIAZ J.、ALINS J.、SILVA-CARDENAS C. 和 BARTRA-GARDINI G. RAR：车辆网络的风险感知撤销机制。《2012 年 IEEE 第 75 届车辆技术会议（VTC 春季）》论文集，2012: 1-5 。https://doi.org/10.1109/vetecs.2012.6239941。

[27] KONDAREDDY Y.、DI CRESCENZO G. 和

AGRAWAL P. 车载网络证书撤销列表分发协议分析。2010 年 IEEE 全球电信会议 (GLOBECOM 2010) 论文集，2010: 1-5。https://doi.org/10.1109/glocom.2010.5683985。

[28] CHEN J., CAO X., ZHANG Y., XU W., 和 SUN Y.。车联网中移动辅助证书撤销列表分发的性能测量。无线通信与移动计算，2011，11(7): 888-898。https://doi.org/10.1002/wcm.858。

[29] LEQUERICA I.、MARTINEZ J. A. 和 RUIZ P. M. 利用下一代网络 (NGN) 功能在车载网络中高效实现证书撤销。2010 年 IEEE 第 72 届车载技术会议论文集 - 2010 年秋季：1-5 页。https://doi.org/10.1109/vetecf.2010.5594232。

[30] QI J. 和 GAO T. 一种用于车联网的隐私保护身份验证和假名撤销方案。IEEE 访问，2020，8：177693-177707。https://doi.org/10.1109/access.2020.3027718。

[31] RABIEH K.、PAN M.、HAN Z. 和 FORD V. SRPV：一种基于假名的车载自组织网络可扩展撤销方案。2018 年 IEEE 国际通信会议 (ICC) 论文集，2018，1-6 页。https://doi.org/10.1109/icc.2018.8422736。

[32] SUN Y.、FENG Z.、HU Q. 和 SU J. 一种用于车联网中基于群签名匿名认证的高效分布式密钥管理方案。安全与通信网络，2011，5(1): 79-86。https://doi.org/10.1002/sec.302。

[33] 。 YANG A., WENG J., YANG K., HUANG C., 和 SHEN X. 将身份验证委托给边缘：一种面向车辆网络的去中心化身份验证架构。IEEE 智能交通系统学报，2022, 23(2): 1284–1298 。https://doi.org/10.1109/tits.2020.3024000。

[34] WANG Q., GAO D., 和 CHEN D. 车辆网络中的证书撤销方案：一项综述。IEEE 访问，2020, 8: 26223–26234。https://doi.org/10.1109/access.2020.2970460。

[35] HICKS C., 和 GARCIA F. D. 一种用于 V2X 中不可链接 ECDSA 假名的车辆 DAA 方案。 2020 年 IEEE 欧洲安全与隐私研讨会 (EuroS&P)， 2020： 460–473。https://doi.org/10.1109/eurosp48549.2020.00036。

[36] VERHEUL E.、HICKS C. 和 GARCIA F. D. IFAL：为 V2X 颁发先激活后证书。2019 年 IEEE 欧洲安全与隐私研讨会 (EuroS&P)， 2019： 279–293。https://doi.org/10.1109/eurosp.2019.00029。

[37] SANTESSON S.、MYERS M.、ANKNEY R.、MALPANI A.、GALPERIN S. 和 ADAMS C. X.509 互联网公钥基础设施在线证书状态协议 - OCSP。RFC 编辑，2013。https://doi.org/10.17487/rfc6960。

[38] SIMPLICIO M. A.、COMINETTI E. L.、KUPWADE PATIL H.、RICARDINI J. E. 和 SILVA M. V. M. 车载公钥基础设施中的撤销：平衡隐私与效率。《车载通信》，2021，28: 100309。https://doi.org/10.1016/j.vehcom.2020.100309。

[39] LARSEN B.、GIANNETSOS T.、KRONTIRIS I. 和 GOLDMAN K. 道路上的直接匿名证明：C-ITS 中高效且保护隐私的撤销。第 14 届 ACM 无线和移动网络安全与隐私会议论文集，2021： 48–59 页。https://doi.org/10.1145/3448300.3467832

[40] SANDHU R. 基于密码学的车载自组织网络安全。《国际应用科学与工程技术研究杂志》，2023，11(6): 1006‑1013。https://doi.org/10.22214/ijraset.2023.53739

[41] FÖRSTER D.、LÖHR H.、ZIBUSCHKA J. 和 KARGL F. REWIRE‑无解析撤销：一种适用于车载自组织网络的隐私友好型撤销机制。《信任与可信计算》，2015，193‑208。https://doi.org/10.1007/978-3-319-22846-4_12。

[42] WHITEFIELD J.、CHEN L.、KARGL F.、PAVERD A.、SCHNEIDER S.、TREHARNE H. 和 WESEMEYER S. V2X 撤销协议的形式化分析。安全与信任管理，2017：147‑163 页。https://doi.org/10.1007/978-3-319-68063-7_10。

[43] LINDEMER S. 物联网数字证书撤销。 2019。https://www.diva-portal.org/smash/get/diva2:1331631/FULLTEXT01.pdf。

[44] ISLAM, N. 车载自组织网络中的证书撤销：一种新方法。国际网络系统与安全会议（NSysS）论文集，2016：1-5。https://doi.org/10.1109/nsyss.2016.7400703。

Word count: 5,809 words, excluding references.

Peer review information:
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 3 reports
Number of revision rounds: 2 rounds
Final revised version submitted: April 27, 2025