IEICE Communications Express, Vol.13, No.4, 134–137

ComEX

LETTER

Efficient distribution of CRL with grouping method in V2X communication

Sasuke Nishikawa[1, a)] **and Kenya Sato**[1]

Abstract In the realm of V2X (Vehicle to Everything) communication research, privacy is upheld through the use of pseudonym technology. However, employing pseudonyms necessitates the distribution of Certificate Revocation Lists (CRLs), posing challenges as the CRL size grows with the increase in invalidated pseudonyms, congesting communication bandwidth. To address this, our proposed method distributes CRLs exclusively to a lead vehicle, tasked with validating pseudonyms for nearby vehicles. Simulation results demonstrate the efficacy of our approach, reducing communication traffic and maintaining delays below 100ms. The proposed technique effectively mitigates the challenges associated with pseudonym-based CRL distribution in V2X communication.

Keywords: CRL, grouping method, pseudonym
Classification: Network system

1. Introduction

In recent years, extensive research has focused on Vehicle-to-Everything (V2X) communication, anticipated to enhance traffic safety and efficiency by preventing accidents and alleviating congestion. However, security and privacy concerns arise from exchanging various vehicle information, such as position, speed, and direction, among nearby vehicles using the vehicle's ID, posing challenges related to easy tracking.

One proposed solution involves implementing pseudonyms—vehicle IDs that change at regular intervals—to render tracking difficult. In this approach, a pseudonym authentication authority invalidates pseudonyms for vehicles exhibiting improper behavior or facing issues, ensuring secure communication. The invalidated pseudonyms, along with their corresponding vehicle IDs, are disseminated to other vehicles through a Certificate Revocation List (CRL). Each vehicle, when engaging in communication with others, verifies the legitimacy of pseudonyms using the CRL, trusting messages only from vehicles with valid pseudonyms [1].

However, the pseudonym change approach faces challenges as the number of invalidated pseudonyms increases, leading to larger CRL sizes and longer distribution times, hindering proper pseudonym validation. Additionally, CRL distribution congests communication bandwidth, affecting other applications. Hence, there is a need to explore methods for distributing CRL with minimal communication traffic, ensuring real-time tracking of invalidated pseudonyms.

[1] Graduate School of Science and Engineering, Doshisha University, Japan
[a)] sasuke.nishikawa@nislab.doshisha.ac.jp

DOI: 10.23919/comex.2024XBL0006
Received January 12, 2024
Accepted January 29, 2024
Publicized February 16, 2024
Copyedited April 1, 2024

2. Related technology

2.1 Pseudonym

One method to protect location privacy is through the use of pseudonyms. Pseudonyms are temporary identifiers assigned to V2X communication devices to make tracking the specific location information of a vehicle difficult. The essence of pseudonyms lies in the certificates issued by a Pseudonym Certification Authority (PCA) as depicted in Fig. 1 [2]. In the issuance process, a vehicle registers its information with a Long-Term Certification Authority (LTCA), requests the issuance of a Long-Term Certification (LTC), and receives it from the LTCA. Subsequently, using the LTC, the vehicle requests the issuance of a Pseudonym Certificate (PC) from the PCA. The PCA, upon receiving the request, consults the LTCA about the associated LTC. If the provided LTC is correct, the PCA issues the PC. Additionally, pseudonyms may expire due to factors such as reaching their validity period, the vehicle engaging in improper behavior, or experiencing malfunctions due to troubles, among other reasons

2.2 CRL

There is a method to validate the effectiveness of pseudonyms using a list of invalidated pseudonyms called Certificate Revocation Lists (CRL) distributed by the Pseudonym Certification Authority (PCA). The verification procedure for pseudonym effectiveness is illustrated in Fig. 2. Initially, the PCA distributes the CRL to all vehicles. Subsequently, each vehicle utilizes its pseudonyms to communicate with surrounding vehicles. If, during this communication, pseudonym B is listed in the CRL, the re-

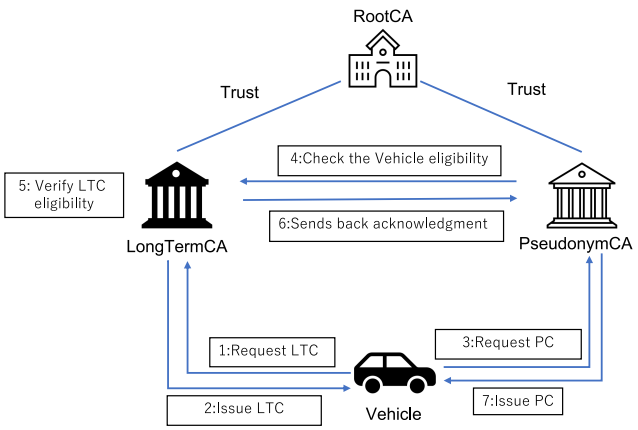

Fig. 1 Procedure for issuing a pseudonym

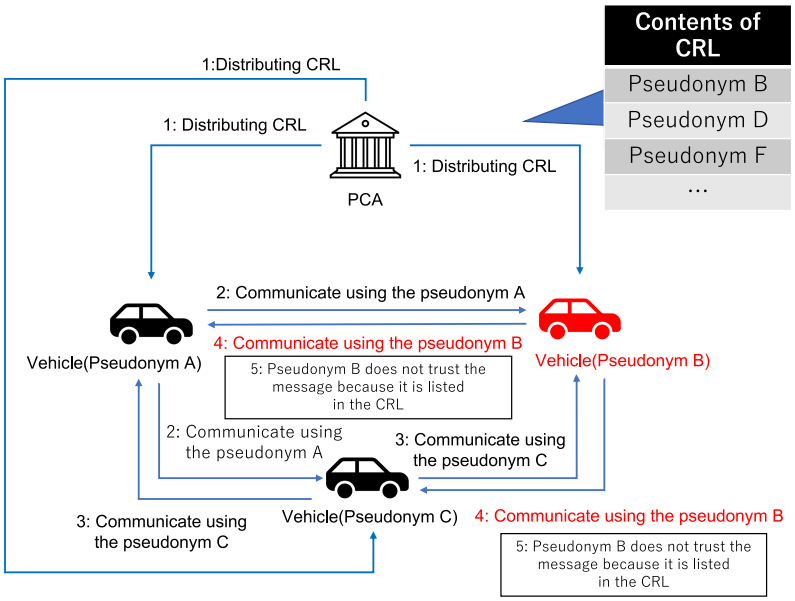

Fig. 2 Procedures for validating pseudonyms using CRL

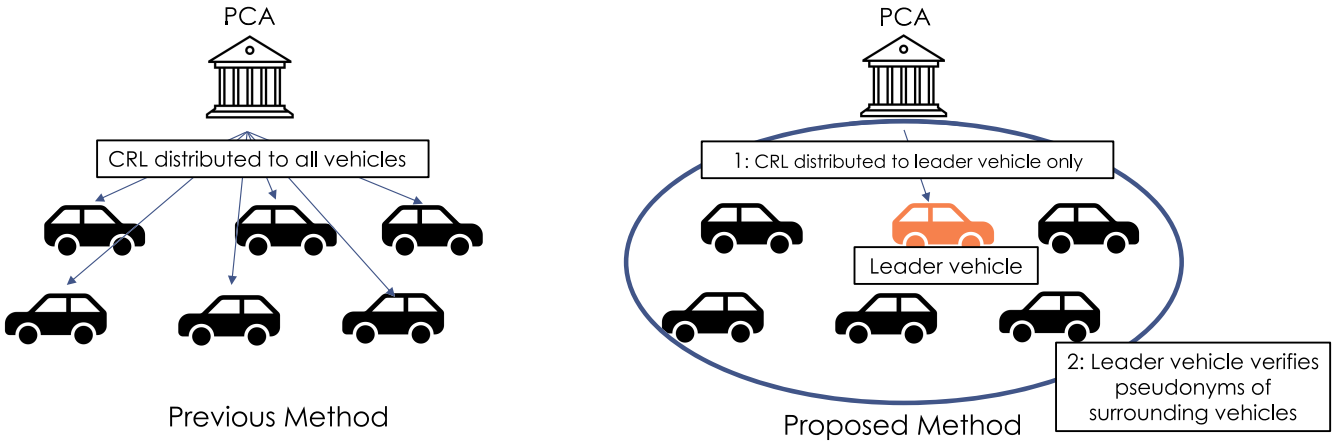

Fig. 3 Overview of the proposed method

ceiving vehicle does not trust messages using pseudonym B. Therefore, each vehicle must maintain an up-to-date version of the CRL it possesses.

However, as the number of invalidated pseudonyms increases, the data size of the CRL grows, potentially congesting communication bandwidth. Congestion in communication bandwidth can result in delayed CRL updates and may impact the communication of other applications.

3. Proposal method

3.1 Overview

In this study, the use of leader vehicles is proposed to temporarily group multiple vehicles, aiming to reduce the communication traffic for Certificate Revocation List (CRL) distribution and identify vehicles using expired pseudonyms. The overview of the proposed method is illustrated in Fig. 3. Without the proposed method, distributing CRL to all vehicles on the road results in high communication traffic. In contrast, the proposed method distributes CRL only to leader vehicles, effectively reducing communication traffic. Additionally, the leader vehicle disseminates only the differences between its CRL and the latest version.

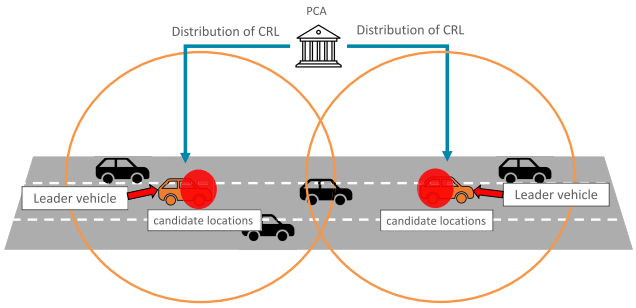

Fig. 4 How to determine the leader vehicle

3.2 Vehicles

In this study, vehicles are considered as nodes engaged in V2X communication. They broadcast messages at regular intervals, including pseudonyms, position, speed, direction, and vehicle ID. Among these vehicles, one leader vehicle is determined within geographically defined zones.

3.3 Leader vehicles

Leader vehicles receive the Certificate Revocation List (CRL) from the Pseudonym Certification Authority (PCA) and are responsible for validating pseudonyms included in messages received from other vehicles. The validation results for pseudonyms are broadcasted in real-time to surrounding vehicles. The method for determining leader vehicles is referenced from [3]. The PCA places potential candidate locations for leader vehicles uniformly on the map, as illustrated in Fig. 4, and designates the closest vehicle to that location as the leader vehicle.

3.4 PCA

The PCA distributes the CRL to each leader vehicle whenever pseudonyms expire and CRL is updated. The locations for determining leader vehicles are predefined in advance. The PCA instructs the vehicle closest to these predefined locations to become the leader and send the difference between the latest CRL and the CRL held by that vehicle. In this study, it is assumed that the authentication authority is aware of the timing at which all vehicles possess their CRL.

3.5 The operational procedure

The operational procedure is outlined below:

1. PCA determines the leader vehicle for CRL distribution.
2. PCA distributes CRL to the leader vehicle.
3. The leader vehicle receives the CRL from the PCA.
4. The leader vehicle verifies if the pseudonyms attached to the broadcasted messages from surrounding vehicles exist in the received CRL.
5. If there are expired pseudonyms, the leader vehicle notifies surrounding vehicles.

4. Evaluation

4.1 Overview

In the evaluation, simulations were conducted using the ns3 network simulator. A comparison was made between scenarios using the proposed method and those without it. Evaluation criteria included communication traffic volume during CRL distribution and the delay time until CRL distribution to all vehicles.

4.2 Evaluation scenario

The parameters used during the simulation are presented in Table I. The assumed environment involves determining leader vehicles to ensure all vehicles on the road are within the communication range of leader vehicles, allowing for the verification of all exchanged message pseudonyms. The CRL size is referenced from IEEE1609.2 [4], with 230 bytes for headers and signature parts, and an additional 14 bytes for each revoked pseudonym. Vehicles are uniformly distributed on the map and assumed to be stationary. The number of leader vehicles is determined by dividing the area of the map for simulation by the area covered by the communication range of a vehicle, resulting in 10 leader vehicles for this study.

Table I Evaluation parameters

Parameters	setting
Number of Vehicles	250
V2V Communication Range	300(m)
Map Area	1 (km^2)
Vehicle Message Sending Interval	0.1(s)
Pseudonym Update Frequency	1, 10, 20 (s)
Simulation Time	30(s)

5. Results and discussion

The latency for distributing the CRL to all vehicles until completion is depicted in Fig. 5. The approach of distributing CRL to all vehicles exceeds 500ms, while the method of distributing CRL only to leader vehicles results in a latency below 100ms. One of the latency requirements for V2X communication is a 100ms benchmark, which the proposed method satisfies, indicating its effectiveness.

Next, the communication traffic volume for CRL distribution through simulation, varying with the pseudonym update frequency, is illustrated in Fig. 6. The proposed method demonstrates a reduction in communication traffic volume with higher pseudonym update frequencies. The reduction ratio aligns closely with the proportion of total vehicles to leader vehicles. In actual environments, as CRL is distributed with each leader vehicle selection, the achievable reduction ratio tends to be smaller.

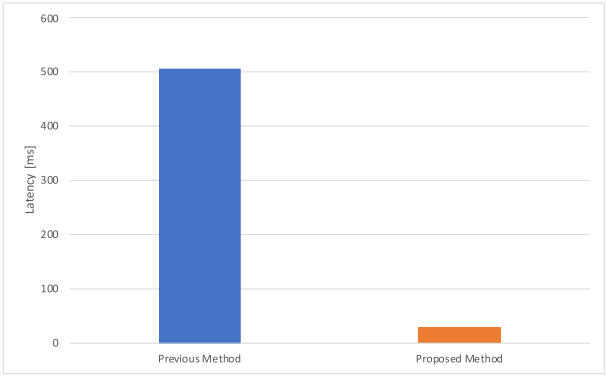

Fig. 5 Latency

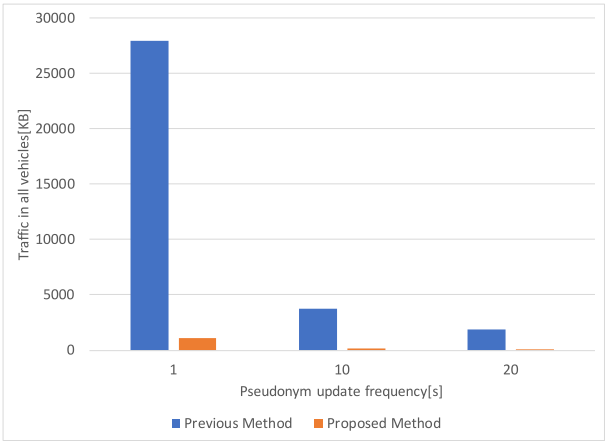

Fig. 6 Traffic

6. Conclusion

In this study, we proposed a method to address the challenge of Certificate Revocation List (CRL) distribution in utilizing pseudonyms for privacy protection in V2X communication. The approach involves distributing CRL to leader vehicles and having them undertake the validation of pseudonym effectiveness for surrounding vehicles, aiming to reduce the communication traffic volume used for CRL distribution. Compared to the method of distributing CRL to all vehicles, this approach is expected to achieve CRL distribution with minimal communication traffic volume and the ability to detect expired pseudonyms. The evaluation results confirmed that our approach effectively reduces communication traffic and exhibits minimal delay in CRL distribution. This suggests that the proposed method is a practical and efficient privacy-preserving solution.

For future perspectives, there are two aspects to consider: reducing the size of CRL and refining the selection of leader vehicles for a more realistic environment. Firstly, to reduce the size of CRL, a method can be implemented to selectively include pseudonyms in the CRL based on the location information of vehicles. Since vehicles that are a certain distance apart do not communicate with each other, there is no need to validate the pseudonyms they can possess. By excluding these pseudonyms from the CRL, the overall size can be reduced. Secondly, for the selection of leader vehicles, placing multiple leader vehicles within the communication range of vehicles is a potential approach. In this study, a single leader vehicle was set within the communication range of vehicles, and this may not function well in cases of leader vehicle malfunctions or unauthorized actions. Therefore, selecting multiple leader vehicles allows mutual monitoring among them, enabling better handling of issues such as malfunctions or unauthorized actions.

Acknowledgments

This work was partly supported by JSPS KAKENHI Grant Number JP20H00589

References

[1] ETSI TR 103 415 V1.1.1 (2018-04), “Intelligent transport systems(ITS); Security; Prestandardization study on pseudonym change management,” 2018.
[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 2015. DOI: 10.1109/comst.2014.2345420
[3] M. Dan, Y. Okabe, and H. Shigeno, “A pseudonym change scheme considering vehicle density for preserving location privacy in vehicular network,” *IPSJ SIG-ITS*, vol. 2019-ITS-78, no. 6, pp. 1–6, 2019.
[4] IEEE P1609.2, “Trial-use standard for wireless access in vehicular environments (WAVE) – Security services for applications and management messages,” IEEE, 2006.