Infrastructure-Independent Pseudonym Swap Protocol for Vehicular Networks

Abdueli Paulo Mdee, Muhammad Toaha Raza Khan, Junho Seo, Dongkyun Kim[†]
School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea
[†] *Corresponding Author*
{apmdee, toaha, jhseo, dongkyun}@knu.ac.kr

***Abstract*—Vehicular Ad-hoc Networks (VANETs) are increasingly gaining the attention of academic institutions, governments, and automobile manufacturers due to their prospect to offer safety, traffic efficiency, and infotainment services to drivers and passengers. However, they suffer from location privacy leakage as vehicles must periodically transmit unencrypted beacon messages. One of the techniques proposed to preserve location privacy in the literature is pseudonym swap. However, existing pseudonym swap schemes either depend on Roadside Units (RSUs) or ignore VANET security requirements. Therefore, we propose a new pseudonym swap scheme that addresses the existing issues by using non-swappable and swappable pseudonyms. Moreover, vehicles simultaneously and randomly change pseudonyms soon after swapping, an approach that further enhances privacy in our scheme. The simulation experiments show that our scheme performs better in confusing a tracking adversary than the existing schemes.**

***Index Terms*—Vehicular Ad-hoc Networks (VANETs), Location Privacy, Non-swappable and Swappable Pseudonyms, RSU independence**

I. Introduction

Vehicular Ad-hoc Networks (VANETs) are types of Mobile Ad-hoc Networks (MANETs) designed for vehicles. VANETs have gained the attention of different stakeholders due to their prospect to offer safety, traffic efficiency, and infotainment services to drivers and passengers [1]. Such services include pre-crash sensing warnings, in-vehicle signage, place of interest (PoI), etc. VANETs comprise Roadside Units (RSUs) and vehicles equipped with On-Board Units (OBUs) to perform vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. RSUs and vehicles communicate wirelessly using Dedicated Short-Range Communications (DSRC) technology.

To support the services, VANETs require vehicles to broadcast beacon messages at a rate ranging from 1 Hz to 10 Hz [2]. The beacon messages contain vehicles' information such as position, velocity, timestamp, identity, signature, etc. Despite their high time resolution, beacon messages are not encrypted due to stringent latency requirements of some safety applications [3]. Therefore, anyone can easily overhear beacon messages and track vehicles in real-time resulting in violation of location privacy. The violation can facilitate other attacks such as burglary, road accidents planning, kidnapping, assassination, stalking, etc.

Researchers have proposed different privacy-preserving schemes in the literature to address the location privacy issue in beacon messages. The predominant way accepted by IEEE and ETSI is using pseudonyms instead of vehicles' real identities and changing them accordingly [4]. Pseudonyms are public keys signed by the Certificate Authority (CA) and do not contain the identity of any vehicle. Authors in [5], [6] proposed using designated areas along the road called mix-zones for vehicles to change pseudonyms when passing, whereas in [7] vehicles dynamically create mix-zones at any place and time. In [8], authors used a silent period whereby vehicles halt, for a while, the transmission of beacon messages when changing pseudonyms. Authors in [9] proposed vehicles enter the silence at low speed (below 30 km/h) to minimize the negative impacts of silence on the performance of safety applications. However, these schemes require vehicles to be preloaded with many pseudonyms during the registration at the CA. Consequently, they impose high computation and storage overheads on the CA and suffer high communication overheads when revoking vehicles as their number grows [10].

To address the stated problems, other researchers suggested vehicles swap pseudonyms hence vehicles can be preloaded with less few pseudonyms. In [11], [12], each vehicle get one pseudonym after registration. To protect location privacy, a vehicle exchanges its pseudonym with another vehicle via the RSUs, and new mapping information is sent to the CA to ensure accountability. For enhanced location privacy, a vehicle in [11] does an exchange when it meets a trigger while in [12] vehicles exchange based on pseudonym-indistinguishability. In other schemes [13], [14], each vehicle gets a time-slotted pseudonym pool of fixed size. Afterward, a vehicle uses one pseudonym for each time slot, change and swap it as necessary without RSUs. In [14], the scheme permutation technique is used for privacy enhancement in sparse traffic scenarios. However, these schemes are either dependent on RSUs or ignore the security requirements. Consequently, RSUs deployment cost is high, vehicles must swap pseudonyms in RSUs presence, and the bottleneck effect occurs at RSUs due to an overwhelming number of requests in rush hours. Moreover, security requirements violation results in revocation failures and repudiation attacks.

Therefore we propose a new scheme that uses a pseudonym swap strategy in addition to a pseudonym changing strategy.

978-1-6654-8550-0/22/$31.00 ©2022 IEEE

TABLE I
THE LIST OF NOTATIONS USED IN OUR SCHEME

Notation	Description
VID_i	Vehicle i real identity
PID_i	Non-swappable pseudonym of vehicle i
$SID_{r,i}$	r^{th} swappable pseudonym of vehicle i
$VID_i : (PID_i, SID_{r,i})$	Vehicle i using PID_i as a semi-public identity and $SID_{r,i}$ as a (fully) public identity
$VID_i : (SID_{r,i})$	Vehicle i using $SID_{r,i}$ as a (fully) public identity
t_x	Swap interval
t_c	Change sync interval

We use two types of pseudonyms: (1) non-swappable and (2) swappable to realize security compliant pseudonym swap without RSUs. Hence, in our scheme no revocation failures, reputation attacks, or dependency on RSU. During registration, each vehicle receives one non-swappable pseudonym and a set of swappable pseudonyms. Vehicles use swappable pseudonyms to sign and authenticate beacon messages. To protect location privacy, they exchange and subsequently randomly change swappable pseudonyms. The exchange is done without RSUs using non-swappable pseudonyms. Afterward, vehicles report new vehicle-pseudonym mapping information to the CA soon after connecting to the infrastructure network. Vehicles utilize a secure and reliable transport protocol to deliver the mapping information to the CA. The simulation experiments show that our proposed protocol performs better in confusing a tracking adversary than existing RSU-independent pseudonym swap schemes. Moreover, it complies with VANET security requirements.

In the rest of the paper, we present our proposed scheme and the rationale for using non-swappable and swappable pseudonyms in Section II. We then describe our simulation and discuss performance results in Section III. Finally, we give our conclusion and future work in Section IV.

II. SECURE RSU-INDEPENDENT PSEUDONYM SWAP

In this section, we comprehensively describe our solution for location privacy protection in VANET. We refer to it as RSU-Independent Pseudonym Swap (RIPS). Table I lists notations used in the rest of this paper.

A. System Architecture

The privacy-preserving system architecture envisioned in our solution is shown in Figure 1. It comprises three layers: (1) Service, (2) Infrastructure, and (3) Vehicular layers. The service layer contains the CA having a vehicle-pseudonym mapping database. The CA is assumed to be trusted; thus, we refer to it as Trusted Authority (TA). The TA is the only entity that registers vehicles and provides them with two types of pseudonyms: swappable and non-swappable pseudonyms. Moreover, the TA stores vehicle-pseudonym mapping information to enforce conditional privacy. In the infrastructure layer, there are RSUs only. The only responsibility of RSUs is relaying encrypted messages between vehicles and the TA; consequently, the trustworthiness of RSUs is not required. Lastly, the vehicular layer comprises vehicles. Registered vehicles use pseudonyms instead of their real identities in V2X communications to ensure privacy. Besides that, they swap and change (swappable) pseudonyms to protect their location privacy.

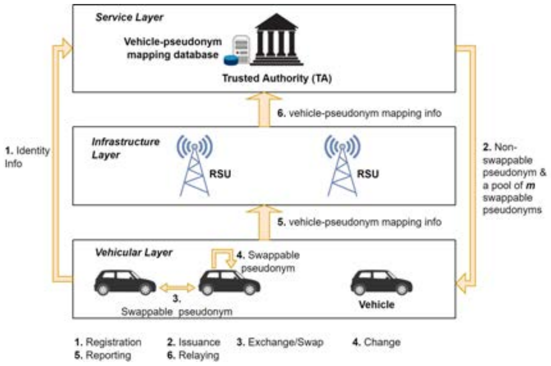


Fig. 1. The privacy preserving system architecture

B. Adversary Model

We consider protecting VANET users' location privacy against a Global Passive Adversary (GPA) [15]. The GPA interest is knowing vehicles' whereabouts by eavesdropping on their beacon messages. This GPA can be realized by either compromising all RSUs or installing low-cost wireless receivers across the VANET to forward (beacon) messages to the GPA tracking server. It tracks vehicles by launching syntactic and semantic pseudonym linking attacks. Although the realization of the assumed GPA is difficult in practice, testing our solution against it proves its strength against less powerful adversaries. We do not consider the GPA using non-vehicular communications tracking mechanisms such as cameras or radio signal patterns.

C. System Initialization

Initially, the TA generates security credentials. Afterward, it registers vehicles providing each with the TA public key, one non-swappable and m swappable pseudonyms. These pseudonyms are public keys signed by the TA, that is, anonymous digital certificates. The TA also provides a private key for each pseudonym given to a vehicle. Subsequently, the TA stores the resulting vehicle-pseudonym mapping information into a mapping database to ensure accountability and non-repudiation. The vehicle-pseudonym mapping information is the association between the vehicle's real identity (presented during registration) and offered pseudonyms.

Hereafter, vehicles use swappable pseudonyms to sign and authenticate beacon messages. On the other hand, they use non-swappable pseudonyms to exchange their swappable pseudonyms while maintaining the accountability and integrity of the mapping database.

D. Attaining Secure RSU Independence

We use swappable and non-swappable pseudonyms to attain RSU-independent pseudonym swap while keeping all security requirements in VANETs. The existing pseudonym swap schemes use one type of pseudonyms that we refer to as swappable pseudonyms. Although this does not create security problems in RSU-dependent pseudonym swap schemes [11] [12], it creates problems in RSU-independent pseudonym swap schemes [13] [14]. We identify two problems: (1) Revocation failure and (2) Inconsistent vehicle-pseudonym mapping database.

The revocation failure problem is a result of a significant delay between the creation of a Certificate Revocation List (CRL) by the TA to revoke a misbehaving vehicle and the dissemination of the CRL to VANET users. The inconsistent mapping database problem occurs when the same pseudonym is swapped by at least two vehicles. Afterward, the vehicles send new mapping information to the TA before the old one. Consequently, the TA incorrectly associates reported pseudonyms with vehicles' real identities. In particular, upon receiving the mapping information, the TA uses it to query the mapping database for the most recent owners of the pseudonyms. Then, the TA uses the query results to insert new mapping information. Therefore, the database becomes inconsistent if the new mapping information is reported before the old one. Figures 2 and 3 show the two problems and our solution that uses swappable and non-swappable pseudonyms.

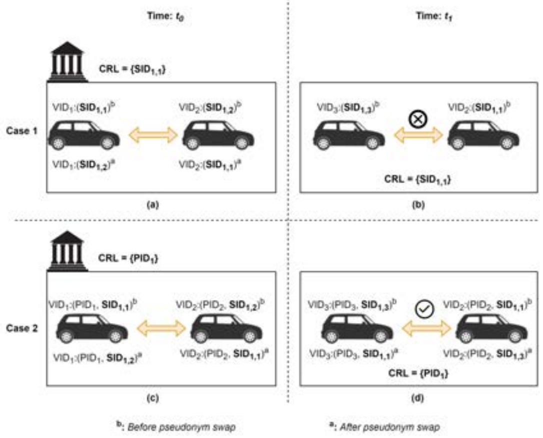
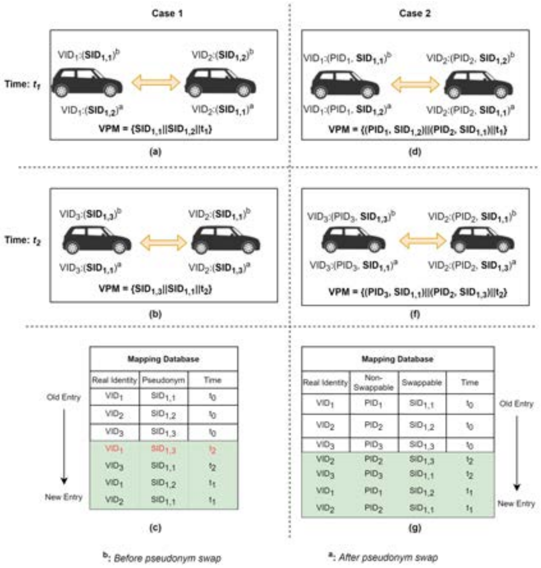

Time: t_0
Time: t_1
CRL = {$SID_{1,1}$}
Case 1
VID_1:($SID_{1,1}$)^b
VID_2:($SID_{1,2}$)^b
VID_1:($SID_{1,2}$)^a
VID_2:($SID_{1,1}$)^a
(a)
VID_3:($SID_{1,3}$)^b
VID_2:($SID_{1,1}$)^b
CRL = {$SID_{1,1}$}
(b)
CRL = {PID_1}
Case 2
VID_1:(PID_1, $SID_{1,1}$)^b
VID_2:(PID_2, $SID_{1,2}$)^b
VID_1:(PID_1, $SID_{1,2}$)^a
VID_2:(PID_2, $SID_{1,1}$)^a
(c)
VID_3:(PID_3, $SID_{1,3}$)^b
VID_2:(PID_2, $SID_{1,1}$)^b
VID_3:(PID_3, $SID_{1,1}$)^a
VID_2:(PID_2, $SID_{1,3}$)^a
CRL = {PID_1}
(d)
^{b}: Before pseudonym swap
^{a}: After pseudonym swap

Fig. 2. In both cases, the vehicle to be revoked *VID*$_1$ exchange its pseudonym with *VID*$_2$ at time t_0 before the distribution of the CRL. Consequently, *VID*$_2$ is revoked in case 1 at time t_1 after the distribution of the CRL; however, it is not so in case 2 where vehicles use swappable and non-swappable pseudonyms.

E. RIPS Algorithm

Each registered vehicle has one non-swappable pseudonym plus m swappable pseudonyms. The m swappable pseudonyms' lifetime overlap contrary to that of a time-slotted pseudonym pool [13]. This overlap provides flexibility in using pseudonyms and makes it difficult for the adversary to predict the next pseudonym. While the vehicle use swappable pseudonyms to sign and authenticate beacons messages, it uses the non-swappable pseudonym to exchange currently used swappable pseudonym with the neighbor.


Case 1
Case 2
Time: t_1
VID_1:($SID_{1,1}$)^b
VID_2:($SID_{1,2}$)^b
VID_1:($SID_{1,2}$)^a
VID_2:($SID_{1,1}$)^a
VPM = {$SID_{1,1}$||$SID_{1,2}$||t_1}
(a)
VID_1:(PID_1, $SID_{1,1}$)^b
VID_2:(PID_2, $SID_{1,2}$)^b
VID_1:(PID_1, $SID_{1,2}$)^a
VID_2:(PID_2, $SID_{1,1}$)^a
VPM = {(PID_1, $SID_{1,2}$)||(PID_2, $SID_{1,1}$)||t_1}
(d)
Time: t_2
VID_3:($SID_{1,3}$)^b
VID_2:($SID_{1,1}$)^b
VID_3:($SID_{1,1}$)^a
VID_2:($SID_{1,3}$)^a
VPM = {$SID_{1,3}$||$SID_{1,1}$||t_2}
(b)
VID_3:(PID_3, $SID_{1,3}$)^b
VID_2:(PID_2, $SID_{1,1}$)^b
VID_3:(PID_3, $SID_{1,1}$)^a
VID_2:(PID_2, $SID_{1,3}$)^a
VPM = {(PID_3, $SID_{1,1}$)||(PID_2, $SID_{1,3}$)||t_2}
(f)
Old Entry
New Entry
(c)
(g)
^{b}: Before pseudonym swap
^{a}: After pseudonym swap

Mapping Database

Real Identity	Pseudonym	Time
VID_1	$SID_{1,1}$	t_0
VID_2	$SID_{1,2}$	t_0
VID_3	$SID_{1,3}$	t_0
VID_1	$SID_{1,3}$	t_2
VID_3	$SID_{1,1}$	t_2
VID_1	$SID_{1,2}$	t_1
VID_2	$SID_{1,1}$	t_1

Mapping Database

Real Identity	Non-Swappable	Swappable	Time
VID_1	PID_1	$SID_{1,1}$	t_0
VID_2	PID_2	$SID_{1,2}$	t_0
VID_3	PID_3	$SID_{1,3}$	t_0
VID_2	PID_2	$SID_{1,3}$	t_2
VID_3	PID_3	$SID_{1,1}$	t_2
VID_1	PID_1	$SID_{1,2}$	t_1
VID_2	PID_2	$SID_{1,1}$	t_1

Fig. 3. The mapping information *VPM* at time t_2 is reported before that of time t_1 for both cases. Consequently, it results in invalid entry (a row with red texts) in the mapping database in case 1; however, no invalid entry in case 2 where vehicles use swappable and non-swappable pseudonyms. The white rows in (c) and (g) are initial mapping information while rows with green background are reported mapping information.

The exchange of currently used swappable pseudonyms is profitable if done in a mix-context where the spatiotemporal information of vehicles is highly correlated. Moreover, the simultaneous pseudonym change by vehicles is highly effective against syntactic linking attacks [8]. Therefore, we determine the mix-context by leveraging position, velocity, and heading information periodically transmitted in beacon messages. We also employ change sync interval (t_c) to synchronize the pseudonym change operation in neighboring vehicles. In particular, each vehicle keeps a list of neighbors that satisfy the mix-context [11]. However, in our solution, we take a neighbor that will maintain the heading and the position thresholds for t_c. Consequently, we eliminate a threshold on the relative velocity.

A vehicle sends a swap request or receives the swap request if it has used its current pseudonym for at least a swap interval (t_x). The requesting vehicle then carries the following steps:

1) It checks whether the number of neighbors in the list is at least the threshold. If not, it waits for a while and repeats step 1; otherwise, it proceeds.
2) It randomly picks a neighbor from the list as its swap partner, encrypts the request using the swap partner's swappable pseudonym, signs the request, and broadcasts it.
3) It sets to change its currently used pseudonym after t_c.
4) It proceeds to exchange with the swap partner.
5) After t_c, it updates its set of m swappable pseudonyms if

it successfully exchanged its currently used pseudonym.

6) It randomly picks from its set of m swappable pseudonyms one pseudonym to be its current pseudonym.
7) It sets to repeat step 1 after time $n \times t_x : n \in \mathbb{R}, n > 1$. n is a request delaying factor, and setting $n > 1$ minimizes contention in sending requests and increases the chance for other vehicles to swap their pseudonyms.

A neighbor of the requesting vehicle performs the following steps:

1) If it has used the current pseudonym for at least t_x, it receives the request; otherwise, it discards it.
2) If it receives the request, it verifies it and checks whether it is the neighbor of the requesting vehicle. If not so, it terminates the process; otherwise, it sets to change its currently used pseudonym after t_c.
3) It tries to decrypt the request.
4) If it succeeds in decrypting the request, it proceeds to exchange with the requesting vehicle; otherwise, it waits for t_c. During waiting, it refrains from receiving any other request.
5) After t_c, it updates its set of m swappable pseudonyms if it successfully exchanged its currently used pseudonym.
6) It randomly picks from its set of m swappable pseudonyms one pseudonym to be its current pseudonym.
7) If it did not exchange its pseudonym, it sets to send swap requests after time t_x; otherwise, it sets to send after $n \times t_x : n \in \mathbb{R}, n > 1$.

All swap messages are encrypted using receiving vehicle's non-swappable pseudonym. However, the swap request is encrypted using receiving vehicle's swappable pseudonym since the requesting vehicle does not know the swap partner's non-swappable pseudonym at the moment of requesting. Lastly, vehicles that exchange their pseudonyms must report the new mapping information to the TA soon after exchanging.

III. Simulation and Performance Evaluation

In this section, we present the simulation of our proposed scheme and discuss its performance results. We also compare our scheme performance with that of SlotSwap [13].

A. Simulation Setup

We implemented our proposed scheme on the NS3 simulator. In addition, we implemented a Global Passive Adversary (GPA) model and a tracking analytic model. The GPA model uses a version of multiple hypothesis tracking (MHT) mechanisms [16] to keep track of vehicles before and after swapping and changing pseudonyms. The GPA has eavesdropping stations spanning the whole geographic area of interest to overhear vehicles' beacon messages. Each time the GPA model tracks vehicles, it sends the results to the tracking analytic model. Similarly, vehicles report their new and old pseudonyms whenever they swap or change. The tracking analytic model then processes the data and output the tracking statistics.

TABLE II
Simulation Parameters

Parameter	Value
Tools	NS3, SUMO, OpenStreetMap
Map	Munich city (2 km x 1.7 km)
MAC layer	802.11p
Beacon rate	10 Hz
Simulation time	450 s – 720 s
Vehicle communication range	350 m
Eavesdropper communication range	250 m
Eavesdropper overlap	100 m
Swap interval	30 s
Request delaying factor	2
Change sync interval	3 s
Change interval (SlotSwap)	60 s
Swappable pseudonyms per vehicle	14
Neighbors threshold	2
Heading	30 degree
Distance threshold	30 m
Number of vehicles	50, 100, 150, 200, 250, 300

Using SUMO, we generated vehicular mobility models on the Munich city map (Figure 4) that we used in our simulation. The mobility models are of different traffic densities with duration ranging from 7.5 min to 12 min. Table 2 lists our simulation parameters.

Fig. 4. Munich city open street map

We evaluate the performance of our proposed scheme in terms of linked pseudonyms ratio, average entropy, and pseudonym changes per vehicle. The linked pseudonyms ratio [17] expresses the confusion a preserving mechanism imposes on an adversary in linking pseudonyms. The lower the ratio, the higher the confusion which translates into higher location privacy. We calculate the ratio using equation 1. $Ratio_{LP}$ is the linked pseudonyms ratio, N_{LP} is the number of linked pseudonyms, and N_{TPC} is the total number of pseudonym changes per traffic scenario.

$$Ratio_{LP} = \frac{N_{LP}}{N_{TPC}} \tag{1}$$

The entropy metric measures how well an adversary can differentiate the target vehicle from other vehicles in the anonymity set. That is, it measures the randomness of the anonymity set. The higher the entropy, the higher the randomness. We calculate the entropy according to [18].

Finally, we study the average number of pseudonyms changed by each vehicle in a scenario. It is assumed that the higher the number of changed pseudonyms, the higher the location privacy. However, that is not always the case [19].

B. Results and Discussion

In Figure 5, the ratio of linked pseudonyms (in percentage) against the number of vehicles for RIPS and SlotSwap is shown. Generally, the ratio decreases as the number of vehicles increases in both schemes because vehicles' spatiotemporal information becomes highly correlated as the number of vehicles increases. However, RIPS outperformed SlotSwap in all scenarios with its ratio decreasing more rapidly as the number of vehicles increases. RIPS performed better because vehicles only swap pseudonyms in a mix-context followed by a simultaneous change of pseudonyms.

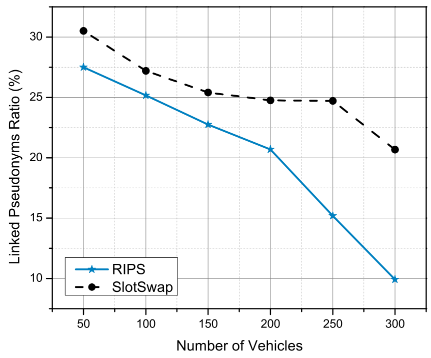


Fig. 5. Linked Pseudonyms Ratio Vs Number of Vehicles

The average entropy for RIPS and SlotSwap is shown in Figure 6. RIPS has higher average entropy than SlotSwap in all traffic scenarios because of the cooperation among neighboring vehicles. However, the average entropy slightly decreases as the number of vehicles increases. The slight decrease results from vehicles that recently swapped pseudonyms refraining from sending swap requests to minimize contention. Hence, more vehicles refrain at the same time as the traffic density increases.

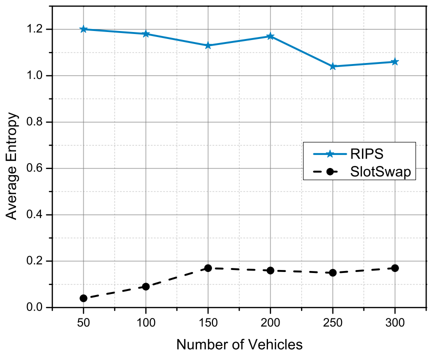


Fig. 6. Average Entropy Vs Number of Vehicles

The average number of pseudonyms changed by each vehicle in different traffic scenarios is depicted in Figure 7 for RIPS and SlotSwap. It increases with the increase in the number of vehicles. RIPS has a lower number than SlotSwap in all scenarios since vehicles do not swap or change pseudonyms except in a mix-context. Moreover, the number is less than one for RIPS in a traffic scenario having 50 vehicles which imply that more than half of vehicles did not swap or change pseudonyms.

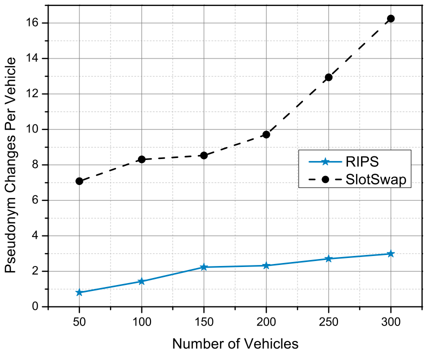


Fig. 7. Pseudonym Changes Per Vehicle Vs Number of Vehicles

IV. Conclusions

Pseudonym swap is one of the proposed techniques to preserve location privacy in VANET. However, existing pseudonym swap schemes either depend on RSUs or ignore VANET security requirements. In this paper, a new pseudonym swap scheme is proposed that addresses existing issues by using non-swappable and swappable pseudonyms. Furthermore, the proposed scheme allows neighboring vehicles to simultaneously change pseudonyms after swapping, which results in enhanced location privacy. The scheme presented a high level of location privacy, especially in dense traffic scenarios. In addition, the scheme preserved all VANET security requirements and did not depend on RSUs to swap pseudonyms. In the future, we would like to further improve and analyze the performance of our scheme by designing an efficient pseudonym swap mechanism, defining a mix-context with a potentially high level of privacy, and carrying out extensive simulations.

Acknowledgment

This research was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT), (NRF-2022R1A2C1003620). In addition, it was supported by the BK21 FOUR project (AI-driven Convergence Software Education Research Program) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (4199990214394).

References

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[2] D. Eckhoff and C. Sommer, "Driving for big data? privacy concerns in vehicular networking," *IEEE Security Privacy*, vol. 12, no. 1, pp. 77–79, 2014.

[3] M. Bradbury, P. Taylor, U. I. Atmaca, C. Maple, and N. Griffiths, "Privacy challenges with protecting live vehicular location context," *IEEE Access*, vol. 8, pp. 207465–207484, 2020.

[4] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[5] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Privanet: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3209–3218, 2020.

[6] M. Khodaei and P. Papadimitratos, "Cooperative location privacy in vehicular networks: Why simple mix zones are not enough," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7985–8004, 2021.

[7] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms - ideal and real," in *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pp. 2521–2525, 2007.

[8] L. Benarous, S. Bitam, and A. Mellouk, "Cslpps: Concerted silence-based location privacy preserving scheme for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7153–7160, 2021.

[9] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE Vehicular Networking Conference (VNC)*, pp. 1–8, 2009.

[10] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas, and A. Nix, "Optimized certificate revocation list distribution for secure v2x communications," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–7, 2017.

[11] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in vanets," *Peer-to-Peer Networking and Applications*, vol. 11, no. 3, pp. 548–560, 2018.

[12] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, and X. Huang, "Papu: Pseudonym swap with provable unlinkability based on differential privacy in vanets," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11789–11802, 2020.

[13] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, 2011.

[14] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "Cpesp: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in vanets," *Vehicular Communications*, vol. 20, p. 100183, 2019.

[15] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[16] D. Reid, "An algorithm for tracking multiple targets," *IEEE Transactions on Automatic Control*, vol. 24, no. 6, pp. 843–854, 1979.

[17] L. Benarous, B. Kadri, and S. Boudjit, "Alloyed pseudonym change strategy for location privacy in vanets," in *2020 IEEE 17th Annual Consumer Communications Networking Conference (CCNC)*, pp. 1–6, 2020.

[18] C. Diaz, "Anonymity metrics revisited," in *Dagstuhl Seminar Proceedings*, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.

[19] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms - ideal and real," in *2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring*, pp. 2521–2525, 2007.