Enhancing privacy-preserving in vehicular cloud through an incentive-based strategy

Hassan Mistareehi[1], Matthew Tennyson[1], Haythem Bany Salameh[2,3]
[1]Department of Computer Science and Information Systems, Murray State University, United States
[2]College of Engineering, Al Ain University, Al Ain, United Arab Emirates
[3]Telecommunications Engineering Department, Yarmouk University, Irbid, Jordan

Article Info

Article history:

Received Jan 12, 2024
Revised Feb 28, 2024
Accepted Mar 5, 2024

Keywords:

Intelligent transportation systems
internet of things
Internet of vehicles
Security and privacy
Vehicle ad hoc network

ABSTRACT

The literature has extensively explored vehicle ad hoc networks (VANETs) and vehicular clouds, with a common assumption in these studies being incorporating onboard units (OBUs) in vehicles. OBUs are used to collect and disseminate information between vehicles. Furthermore, numerous studies assume the presence of road infrastructure for communication. Implementing a vehicular cloud can play a vital role in aggregating data on events such as weather conditions, traffic information and accidents. This information is distributed to other vehicles, allowing drivers to make informed decisions and ensure safe driving practices. To protect privacy within the vehicular cloud, pseudonyms serve as a means of communication between vehicles and roadside units (RSU). Numerous existing approaches suggest more frequent updates to vehicle pseudonyms to reduce the likelihood of linking transmitted messages by vehicles. However, some of these strategies overlook situations where vehicle density is low, and vehicles have limited willingness to engage in the pseudonym-changing process. This article introduces an architecture that encourages vehicles to participate in the pseudonym-changing process to enhance vehicle privacy. This is achieved by issuing rewards to vehicles that can be used to access cloud services.

Corresponding Author:

Hassan Mistareehi
Department of Computer Science and Information Systems, Murray State University
1375 Chestnut St, Murray, KY 42071, United State
Email: hmistareehi@murraystate.com

1. INTRODUCTION

With the increasing fascination of consumers and the industry for autonomous vehicles, there has been a substantial increase in interest in the design of internet of vehicles (IoV). According to specific projections, the global IoV market is expected to surpass 200 billion in the next two years [1]–[4]. Consequently, various automobile manufacturers have introduced initiatives and platforms to integrate with IoV services, such as intelligent parking and collision prevention [5]–[8]. In vehicle ad hoc networks (VANETs), vehicles are generally equipped with on-board units (OBU). These OBUs play a crucial role in the exchange of safety messages and their transmission to vehicles within their transmission range or roadside units (RSUs) through wireless communication devices [9]–[11]. In VANETs, a malicious vehicle can potentially impersonate another car or RSU, posing a threat to steal sensitive information from other vehicles. Furthermore, without the ability of vehicles to communicate anonymously, a malicious vehicle could exploit the lack of anonymity to track other vehicles by correlating the messages transmitted. Consequently, ensuring location privacy has become a significant concern in VANETs [7], [12], [13]. Although numerous privacy-preserving techniques have been proposed in the literature, many of them mainly focus on high-density regions of vehicles rather than address concerns in the low-density areas to improve the privacy of vehicles using mix zone schemes (a mix zone is a designated area where vehicles can alter their pseudonymous. Regularly changing these pseudonyms contributes to improved privacy by minimizing the risk of identification through persistent tracking) [14]–[17]. To address this gap and enhance vehicle privacy, we improve the pseudonym-changing process to reduce the likelihood that attackers establish links between vehicle pseudonyms [18]–[20].

The main contributions of this paper can be outlined as:

– We propose an improved privacy-preserving scheme in the vehicular cloud, fostering active participation of vehicles within the mixed-zone region. Our scheme encourages vehicles to participate in the process of changing their pseudo-IDs within the mixed-zone region by providing them with rewards for their contribution. Therefore, vehicle privacy is strengthened, making it difficult for attackers to establish links between vehicle pseudonyms in a mixed-zone region.
– The proposed scheme ensures the integrity and authenticity of the entities and exchanged packets between these entities.

The subsequent sections of the paper follow this structure. Section 2 explores various related works. Subsequently, section 3 introduces our proposed method. Moving forward, section 4 delves into the result and discussion of our approach. Lastly, section 5 provides a summary of the conclusions drawn.

2. RELATED WORKS

Lu *et al.* [21] proposed to implement a mix zone in social places, such as intersections or locations near busy areas, such as shopping malls. An optimal implementation scenario is at intersections with high traffic flow and traffic lights. Numerous slow-moving vehicles are present in such settings, allowing sufficient time to facilitate the pseudonym-changing process. The studies [22]–[26] have leveraged the road infrastructure to facilitate the change of vehicle pseudonyms. In a specific case, as discussed in [23], the concept of a vehicle location privacy zone (VLPZ) is introduced. This zone incorporates two crucial infrastructures, the router and the aggregator, strategically located at both ends of the VLPZ. Their roles involve ensuring the unlinkability of the pseudonym-changing process. When a vehicle arrives at the router within the VLPZ, it ceases to broadcast its basic safety message. The router then assigns a lane to the vehicle in a random manner, prompting it to modify its pseudo-ID before reaching the aggregator. Identifying the specific vehicle becomes challenging since the order of exits differs from the order of entry due to varying residency periods. In [24], the authors used fog computing to offer a service to change pseudonyms for vehicles. In this method, in contrast to the system described in [23], RSUs provide new pseudonyms for every vehicle in the mixed zone. Another approach, as detailed in [25], introduces a pseudonym exchange system based on differential privacy. When a vehicle requires a new alias, it transmits a request message to the RSUs and vehicles in its vicinity.

Additional vehicles seeking a pseudonym alteration proceed by sending matching messages to the RSUs to indicate their desire to engage in the pseudonym exchange. The RSUs gather these requests and apply the pseudonym exchange algorithm to allocate fresh pseudonyms to each vehicle while adhering to principles of differential privacy. Nonetheless, the process accomplishes the pseudonym exchange with RSUs while guaranteeing that the new and old pseudonyms are indistinguishable and unlinked, although at the expense of decreased efficiency due to the computational and communication expenses involved. In [27], the authors proposed a scheme that allows the vehicles to use a certificate from certificate authority (CA) in order to access the security domain within the RSU. The RSU is required to regularly update the public key in the domain., prompting vehicles to adjust their pseudonyms accordingly and ensuring periodic pseudonym changes. However, this approach requires communication between vehicles and the RSU for pseudonym changes, potentially leading to situations where, under specific conditions, vehicles might not change their pseudonyms due to a lack of timely communication with the RSU.

In summary, the above schemes did not address the issue of providing incentives to encourage vehicle participation in the pseudonym-changing process and mitigate selfish behavior. In this paper, we introduce a reward system in which vehicles are incentivized to actively participate in the pseudonym-changing process to improve overall vehicle privacy.

3. THE PROPOSED METHOD

This section presents an overview of both the network model and the proposed secure reward system method, providing essential details about the proposed vehicular cloud architecture and the primary assumptions made in our analysis, along with the framework components. Furthermore, by explaining the abbreviations used throughout the paper, Table 1 improves the understanding of the readers, making it easier to follow the technical aspects discussed in the paper.

Table 1. Notations used in this paper

Notation	Description
ID_A	Identity of Entity A
PID_A	Pseudo-Identity of Entity A
M	A Message
V_a	Vehicle a
ts	Timestamp
PR_A	Private Key of Entity A
PU_A	Public Key of Entity A
K	Shared Secret Key
$SIG_A(M)$	Signature of M Signed with PR_A
$H()$	Hash Function
TA	Trusted Authority
SP	Service Provider
RS	Reward System
OBU	On Board Units
RSU	Roadside Unit
$s\#$	Service Number
$tr\#$	Transaction Number
$proof$	Proof of the work performed
R	Reward
$E(M, K)$	Encryption of M with Key K
CA	Certificate Authority
$Cert_v$	Vehicle v Certificate
$Cert_{RSU}$	RSU Certificate

3.1. System model and assumptions

This section presents the system model and its main components. In addition, we summarize the main assumption used in our analysis. Figure 1 illustrates the proposed architecture of the vehicular cloud. The vehicular cloud structure discussed in this paper includes the following components:

- Trusted authority (TA): The TA resides in the cloud and maintains secure communication channels with the reward system (RS) and service provider (SP). During vehicle registration or renewal, the TA issues a certificate to the vehicle. It is responsible for managing all private information related to vehicles. The TA assists the SP in vehicle verification when necessary. The TA can disclose the real identity of vehicles to legal authorities when investigative actions are mandated.
- Service provider (SP): The role of the SP is to advertise services, negotiate service contracts, validate proofs of work carried out by vehicles, and distribute rewards to encourage their active participation in the pseudonym-changing process.
- Reward system (RS): The RS establishes an account for each registered vehicle, linking the account with the vehicle pseudo-ID. RS assigns rewards to vehicles when they actively participate in the pseudonym-changing process.
- Road side units (RSUs): RSUs are strategically positioned along roads and connected via a network, serving as gateways that enable communication between the vehicular VANET and the cloud.
- On board units (OBUs): An OBU is a device attached to vehicles, equipped with computational, communication, and storage capabilities. In addition, it can verify the reward balance with the RS in the cloud.

The operational assumptions in our design include: the complete trustworthiness of RS and TA, ensuring that they cannot be compromised, along with the assignment of public/private key pairs to vehicles upon vehicle registration, with RS and SP public keys stored in the OBU, enabling secure communication. In addition, vehicles have the ability to establish communication with the cloud through RSUs, facilitating message exchange within the coverage area of each RSU. Specifically, any vehicle located within the coverage area of an RSU can transmit and receive messages to and from that particular RSU.

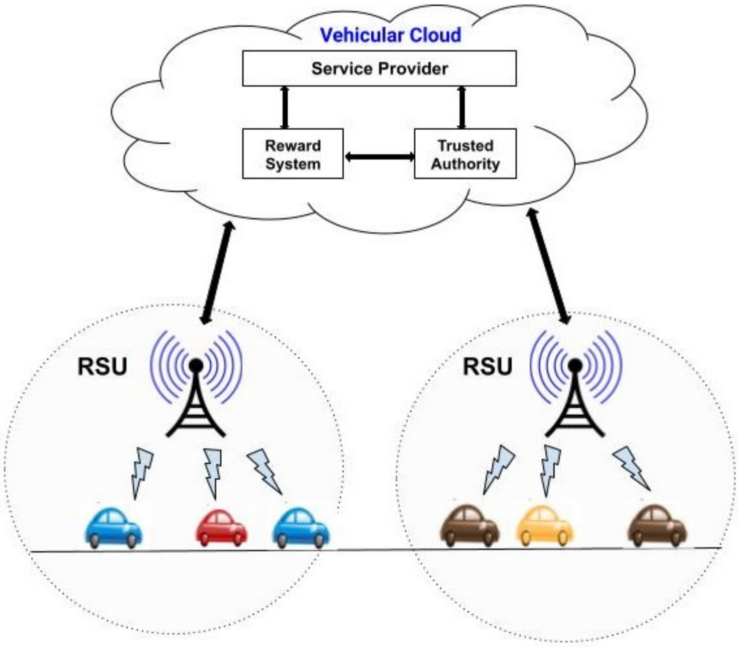

Figure 1. An illustrative system model for a VANET

3.2. The proposed secure reward system

The proposed scheme comprises three key steps: contract initiation, reward request, and reward utilization to access cloud services. In the initial step, vehicles receive an invitation from the cloud's SP via RSUs, authenticate with the TA, and receive a signed contract to start the task, ensuring message authenticity and integrity through encryption and digital signatures. Subsequently, in the reward request step, the vehicle sends proof of completing the task to the SP, triggering a reward request to the RS for compensation, and then shares a transaction number with the SP for confirmation. Finally, vehicles, in the last step, can utilize rewards as payment to access cloud services.

3.2.1. Contract

The SP in the cloud sends a message inviting vehicles to participate in the pseudonym-changing process. Upon receiving this message, a vehicle interested in contributing to the process sends a request message for the task to the SP through the RSUs. Subsequently, the SP collaborates with the TA to verify the vehicle's authenticity. Once validated, the SP generates a signed contract describing the task terms between the vehicle and the service provider. This contract is then transmitted to the vehicle, allowing it to begin the specified work.

In our approach, we use public-key encryption and digital signatures to guarantee the authenticity and integrity of messages. When a sender wants to transmit a message, they attach a digital signature. This digital signature is crafted by encrypting the hash of the message with the sender's private key. As this process is exclusive to the sender, it guarantees the message's authenticity. To ensure integrity, the recipient verifies whether the hash within the digital signature corresponds to the hash of the message computed locally. If these hashes coincide, the recipient can confirm the authenticity and integrity of the transmissions.

The SP sends a message M_1 through the cloud, where,

$$M_1 = ID_{SP}, s\#si, ts, SIG_{SP}$$

where $SIG_{SP} = E(H(s\#si, ts), PR_SP)$.

The message M_1 contains the service number $s\#$ and the cloud service si information that incorporates the SP ID, the reward amount, and the work requirement. In addition, the SP adds a digital signature to the message ($SIG_{SP}(M)$). When a vehicle V receives the message M_1 and opts to participate in the pseudonym exchange process, it initiates a request message M_2, where M_2 is given below, encrypting the si, certificate ($Cert_v$), and timestamp (ts) using the public key SP (PU_{SP}). Upon generating the work request message M_2 (the task of changing its pseudo ID), the vehicle forwards it to the SP in the cloud via a close RSU.

$$M_2 = ID_{SP}, E((PID_V, s\# Cert_v, ts, PU_{SP}), SIG_V$$

where $SIG_V = E(H(PID_V, s\# Cert_v, ts), PR_V)$.

Upon reception of M_2, the SP can authenticate the vehicle by validating its $Cert_v$ and PID_V in collaboration with the TA, followed by decrypting the message. Furthermore, the SP checks whether the vehicle has been revoked (misbehaved). After authenticating the vehicle, the SP creates a message M_3 by appending the contract and its signature SIG_{SP}, as follows:

$$M_3 = PID_V, E((ID_{SP}, contract, ts), PU_V), SIG_{SP}$$

where $SIG_{SP} = E(H(ID_{SP}, contract, ts), PR_{SP})$.

Upon receiving the message M_3, the vehicle initiates the process through transmitting an acknowledgment M_4 to the SP. Subsequently, the vehicle can start participating in the pseudonym-changing process.

$$M_4 = ID_{SP}, E((PID_V, contract, ts), PU_{SP}), SIG_V$$

where $SIG_V = E(H(PID_V, contract, ts), PR_V)$.

3.2.2. Requesting a reward

Following completing the assigned task (participation in the pseudonym-changing process), a vehicle sends a message to the SP containing proof of the completed work. The evidence includes messages transmitted by a vehicle using its recently assigned pseudo-ID. This proof message helps the SP validate the work's successful completion. Upon successful verification, the SP triggers a reward request to the RS, which grants compensation to the vehicle for the completed task. Subsequent to the RS handling the reward request, a transaction number is created and shared with both the SP and the vehicle for confirmation.

After participating in the pseudonym-changing process within a RSU region, the vehicle informs the SP by transmitting a message M_5 containing the proof of the work performed.

$$M_5 = ID_{SP}, E((PID_V, s\#, proof, ts), PU_{SP}), SIG_V$$

where $SIG_V = E(H(PID_V, s\#, proof, ts), PR_V)$.

The proof of participation must be verifiable by the SP. Upon successful verification of participation, the SP generates a reward request message M_6, appended with the digital signature, and transmits it to the RS. This facilitates the issuance of rewards to the vehicle as compensation for the completed participation in the pseudonyms-changing process.

$$M_6 = ID_{RS}, E((s\#, PID_V, R, ts), PU_{RS}), SIG_{SP}$$

where $SIG_{SP} = E(H(s\#, PID_V, R, ts), PR_{SP})$.

After processing the reward request, the RS computes the confirmation messages M_7 and M_8 along with a transaction number $tr\#$ for the SP and the vehicle, respectively, as outlined below:

$$M_7 = ID_{SP}, E((ID_{RS}, s\#, tr\#, ts), PU_{SP}), SIG_{RS}$$

where $SIG_{RS} = E(H(ID_{RS}, s\#, tr\#, ts), PR_{RS})$.

$$M_8 = PID_V, E((ID_{RS}, s\#, tr\#, ts), PU_V), SIG_{RS}$$

where $SIG_{RS} = E(H(ID_{RS}, s\#, tr\#, ts), PR_{RS})$.

3.2.3. Utilizing rewards for cloud services

In the context of vehicular cloud, a variety of services can be accessed through cloud service providers. Although cloud services usually operate on a pay-as-you-go basis, the benefit received from providing resources to the cloud could potentially be used as an alternative form of payment for these services. For example, data managers responsible for parking lots can provide vehicles with information on the availability of parking spaces. In transportation systems, cloud technology facilitates the real-time collection of traffic data. This, in turn, allows dynamic traffic flow redirection and optimization of elements such as traffic signals and dynamic traffic management [28].

Vehicles equipped with OBUs capable of verifying reward balances can efficiently utilize cloud services by using rewards, provided they have a sufficient balance to cover the service costs. A vehicle can efficiently utilize rewards-based cloud services by transmitting a message (M9) to the SP as:

$$M_9 = ID_{SP}, E((PID_V, s\#, R, ts), PU_{SP}), SIG_V$$

where $SIG_V = E(H(PID_V, s\#, R, ts), PR_V)$

Upon receiving the communication from the vehicle, the SP verifies the message's authenticity and sends a request to deduct a reward to the RS, following a procedure akin to the one used for requesting rewards. After confirming the vehicle's authenticity and obtaining approval for the reward deduction, the SP notifies the service provider that the vehicle can now access the cloud service.

4. RESULT AND DISCUSSION

4.1. Simulation setup

In this section, we conduct simulation experiments to demonstrate the efficacy of the proposed secure system. Our study area spans 1,000 by 1,500 meters and involves a network of 25 vehicles. Data packets are standardized at 1 KB in size. We employ two-ray propagation models alongside omni-directional transmissions. Ad hoc on-demand distance vector (AODV) routing protocols facilitate packet routing within the network. The experimental setup includes the simulation parameters outlined in Table 2. The main performance metrics are the packet delivery ratio (PDR), the size of the anonymous set, and the vehicle authentication overhead.

Table 2. Simulation parameters

Parameter	Value
Area	1,000-1,500 meters
Numbers of vehicles	25
Data packet size	1 Kb
Buffer size	1 GB
Channel type	Wireless
Mac protocol type	Mac/802-11
Propagation model	Two ray
Antenna type	Omni antenna
Routing protocol	AODV

4.2. Simulation results

4.2.1. Packet delivery ratio

The study explores the influence of selfish vehicles, those unwilling to participate in the pseudonym-changing process, on the performance evaluation of VANET in the absence of any incentive scheme. As shown in Figure 2, the impact of these non-cooperative vehicles on the PDR is demonstrated. The figure illustrates a decreasing trend in the PDR as the proportion of selfish vehicles increases. Initially, assuming a proportion of 0% selfish vehicles, the PDR reaches nearly 70%. However, if the percentage of vehicles that behave selfishly is 50%, the PDR decreases significantly to only 30%. The figure shows that the PDR decreases as the number of selfish vehicles in the network increases.

4.2.2. Anonymous set size

The size of the anonymous set depends on the number of vehicles involved in the procedure of changing pseudonyms [29]. As the size of the anonymous set increases, the level of confusion for potential attackers also rises. Figure 3 demonstrates the total count of vehicles that simultaneously changed their pseudonyms within the RSU region. Initially, it is assumed that 30% of vehicles are selfish and unwilling to participate in the pseudonym-changing process, but this percentage decreases to 10% after the distribution of rewards. The graph illustrates that as the proportion of selfish vehicles decreases, more vehicles engage in the pseudonym-changing process. This complicates the task for attackers trying to link vehicle pseudonyms. For instance, if there are 10 vehicles in the RSU region and it is time for pseudonym changes as scheduled by the RSU, 7 vehicles will modify their pseudonyms without receiving rewards (10 - (10*30%) = 7). With the introduction of rewards, a greater number of vehicles participate in the process, leading to a reduction in the count of selfish vehicles. Consequently, in this scenario, 9 vehicles will take part (10 - (10*10%) = 9). The size of the anonymous set expands as more vehicles engage in the pseudonym change process.

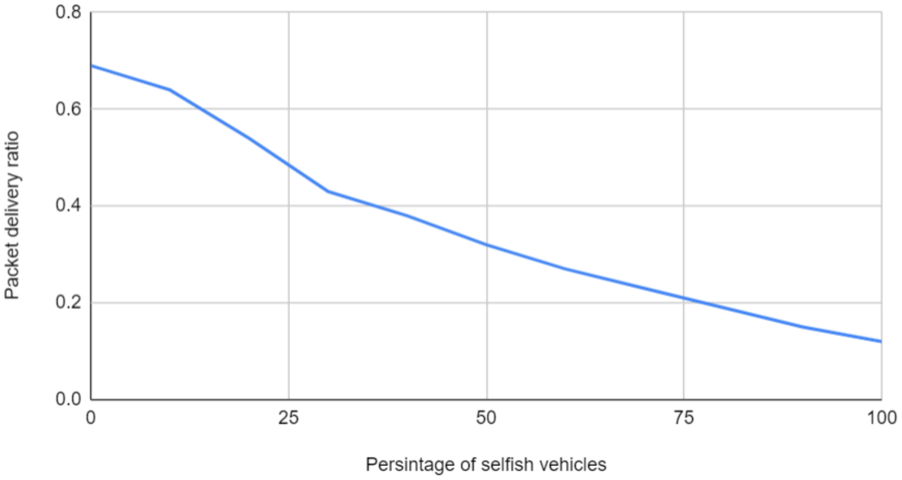

Figure 2. PDR for different percentages of selfish vehicles

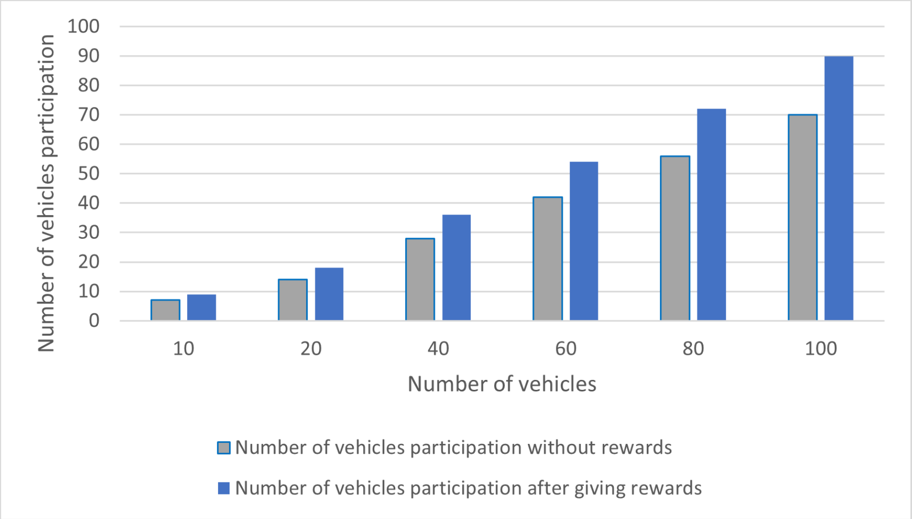

Figure 3. Number of altered pseudonyms in the RSU/GL area

4.2.3. Vehicle authentication overhead

Verifying an Rivest–Shamir–Adleman (RSA) signature on a Toshiba computer equipped with an Intel i3 quad-core processor operating at a clock frequency of 2.50 GHz, running the Windows 8.1 operating system, and having 6 gigabytes of memory requires approximately 0.005 ms in [6]. The computational overhead for different numbers of signatures is shown in Figure 4. Our approach exhibits a slightly higher overhead when rewarding vehicles than in scenarios without rewards. This increased overhead is attributed to the use of the reward system, which improves the privacy of vehicles. For example, when the number of signatures is 90, our scheme's computation overhead is 0.45 ms.

In summary, based on the discussed experimental findings, The PDR decreases as the number of selfish vehicles in the network increases, the size of the anonymous set grows as the number of vehicles participating in the pseudonym-changing process increases, and Our approach exhibits a slightly higher overhead when rewarding vehicles than scenarios without rewarding vehicles for their participation in the pseudonym-changing process. This increased overhead is attributed to the use of the reward system, which improves the privacy of the vehicles. Therefore, our scheme shows that offering incentives to vehicles promotes their participation in the pseudonym-changing process, ultimately enhancing the privacy of vehicles.

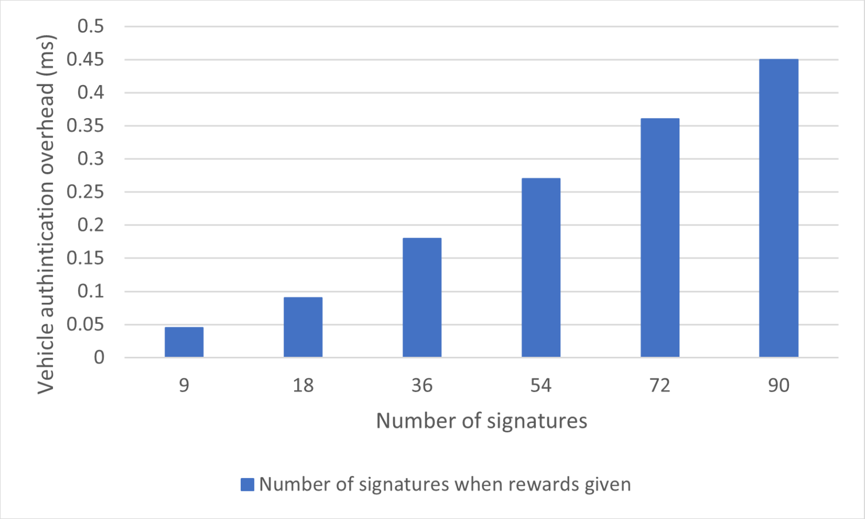

Figure 4. Vehicle authentication overhead

5. CONCLUSION

We have presented an enhanced privacy-preserving scheme for the vehicular cloud, focusing on the participation of vehicles within mixed-zone regions. Our approach relies on mixing zones where vehicles can change their pseudonyms, which complicates the task of linking pseudonyms associated with the same vehicle. By offering rewards, our scheme motivates vehicles to alter their pseudo-IDs, thus enhancing the privacy of vehicles. Furthermore, the proposed scheme guarantees the confidentiality and authentication of the messages. In the future, we plan to conduct real-world experiments and case studies in vehicular environments to assess the effectiveness of privacy-preserving schemes.

REFERENCES

[1] G. Bai, "Optimal design of vehicle structure based on computer-aided technology," *Journal of Electrical and Computer Engineering*, vol. 2022, pp. 1–9, May 2022, doi: 10.1155/2022/3326126.

[2] M. Z. Iskandarani, "Handover between vehicular network providers using bioinspired attractor selection technique," *Journal of Electrical and Computer Engineering*, vol. 2022, pp. 1–13, Mar. 2022, doi: 10.1155/2022/8528313.

[3] J. Yang, Q. Ni, G. Luo, Q. Cheng, L. Oukhellou, and S. Han, "A trustworthy internet of vehicles: the DAO to safe, secure, and collaborative autonomous driving," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 12, pp. 4678–4681, 2023, doi: 10.1109/TIV.2023.3337345.

[4] J. Zheng, J. Shi, Q. He, E. Zhang, A. Hawbani, and L. Zhao, "An influence maximization-based hybrid advertising dissemination for internet of vehicles," *IEEE Networking Letters*, vol. 5, no. 4, pp. 218–222, 2023, doi: 10.1109/lnet.2023.3296081.

[5] N. K. Chaubey and D. Yadav, "Detection of sybil attack in vehicular ad hoc networks by analyzing network performance," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, pp. 1703–1710, 2022, doi: 10.11591/ijece.v12i2.pp1703-1710.

[6] H. Mistareehi and D. Manivannan, "A low-overhead message authentication and secure message dissemination scheme for VANETs," *Network*, vol. 2, no. 1, pp. 139–152, 2022, doi: 10.3390/network2010010.

[7] O. Bouachir, M. Aloqaily, I. Al Ridhawi, O. Alfandi, and H. B. Salameh, "UAV-assisted vehicular communication for densely

crowded environments," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2020, pp. 1–4, doi: 10.1109/NOMS47738.2020.9110438.

[8] H. Elayan, M. Aloqaily, H. B. Salameh, and M. Guizani, "Intelligent cooperative health emergency response system in autonomous vehicles," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, Oct. 2021, pp. 293–298, doi: 10.1109/LCN52139.2021.9524950.

[9] S. Sivakumar, A. Alagumurugan, G. B. B. Vignesh, and S. Dhanush, "Accident analysis and avoidance by V2V communication using lifi technology Li-Fi," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 2, no. 03, pp. 730–733, Mar. 2020.

[10] M. A. Al Noman, M. F. Rahaman, Z. Li, S. Ray, and C. Wang, "A computer vision-based lane detection approach for an autonomous vehicle using the image hough transformation and the edge features," in *Lecture Notes in Networks and Systems*, 2023, vol. 628, pp. 53–66, doi: 10.1007/978-981-19-9888-1_5.

[11] R. V. Chandraiah and A. Ramalingappa, "Secure authentication and data aggregation scheme for routing packets in wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp. 3217–3226, 2023, doi: 10.11591/ijece.v13i3.pp3217-3226.

[12] H. Mistareehi, T. Islam, and D. Manivannan, "A secure and distributed architecture for vehicular cloud," in *Internet of Things (Netherlands)*, Oct. 2021, vol. 13, pp. 127–140, doi: 10.1016/j.iot.2020.100355.

[13] S. Palaniapan and M. A. Kollathodi, "Real time implementation of embedded devices as a security system in intelligent vehicles connected via vanets," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4788–4797, Dec. 2019, doi: 10.11591/ijece.v9i6.pp4788-4797.

[14] K. A. Darabkh, M. S. A. Judeh, H. Bany Salameh, and S. Althunibat, "Mobility aware and dual phase AODV protocol with adaptive hello messages over vehicular ad hoc networks," *AEU - International Journal of Electronics and Communications*, vol. 94, pp. 277–292, 2018, doi: 10.1016/j.aeue.2018.07.020.

[15] C. Dutta and N. Singhal, "Efficient data transmission technique using artificial intelligence in clustered vanet," *Journal of Analysis and Computation (JAC)*, vol. 8, February 2019.

[16] L. Liu, B. Wang, Y. Li, and N. Hu, "Regular vehicle spatial distribution estimation based on machine learning," *Journal of Electrical and Computer Engineering*, vol. 2023, 2023, doi: 10.1155/2023/4954035.

[17] D. M. M. Azzahar, M. Y. Darus, S. J. Elias, J. Jasmis, M. Z. Zakaria, and S. R. M. Dawam, "A review: standard requirements for internet of vehicles (IoV) safety applications," in *2020 5th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Dec. 2020, pp. 1–5, doi: 10.1109/ICRAIE51050.2020.9358383.

[18] K. Chauhan, S. Chidrawar, N. Avhad, M. Gore, and P. A. Jain, "Vehicular emergency system and V2V communication using IOT," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 5, pp. 3260–3263, May 2018.

[19] S. Bai and Z. Zhang, "Anonymous identity authentication scheme for internet of vehicles based on moving target defense," in *2021 International Conference on Advanced Computing and Endogenous Security*, 2021, pp. 1–4, doi: 10.1109/IEEECONF52377.2022.10013357.

[20] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1065–1079, 2018, doi: 10.1109/TITS.2017.2712772.

[21] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, 2012, doi: 10.1109/TVT.2011.2162864.

[22] H. Mistareehi, T. Islam, and D. Manivannan, "A secure and distributed architecture for vehicular cloud," in *Internet of Things (Netherlands)*, Oct. 2021, vol. 13, pp. 127–140, doi: 10.1016/j.iot.2020.100355.

[23] A. Boualouache, S. M. Senouci, and S. Moussaoui, "VLPZ: the vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369–376, 2016, doi: 10.1016/j.procs.2016.04.198.

[24] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2018, doi: 10.1109/TITS.2017.2764095.

[25] X. Li *et al.*, "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, doi: 10.1109/JIOT.2020.3001381.

[26] D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, "Securing vehicular cloud networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 4154–4162, 2019, doi: 10.11591/ijece.v9i5.pp4154-4162.

[27] S. Wang and N. Yao, "LIAP: a local identity-based anonymous message authentication protocol in VANETs," *Computer Communications*, vol. 112, pp. 154–164, 2017, doi: 10.1016/j.comcom.2017.09.005.

[28] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, no. 1, pp. 325–344, 2014, doi: 10.1016/j.jnca.2013.08.004.

[29] X. Li *et al.*, "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, doi: 10.1109/JIOT.2020.3001381.

BIOGRAPHIES OF AUTHORS

Hassan Mistareehi is currently an assistant professor in the Department of Computer Science and Information Systems at Murray State University. He received his Ph.D. degree in computer science from the University of Kentucky. He received his B.S. and M.S. degrees in computer science from Jordan University of Science and Technology, Jordan. His research focuses on the security and privacy of vehicular ad hoc networks (VANET), vehicular cloud (VC), internet of things (IoT), cloud computing, edge computing, ad hoc networks, and sensor networks. He can be contacted at email: hmistareehi@murraystate.com.

Matthew Tennyson earned his B.S. in computer engineering from Rose-Hulman in 1999, then worked at Caterpillar, focusing on embedded systems for earth-moving machinery. He later transitioned to web application development and electrical harness design support at CAT. In 2004, he completed his M.S. in computer science from Bradley while still at Caterpillar. Eventually, he shifted to academia, teaching at Heartland Community College and Midstate College while pursuing a Ph.D. at Nova Southeastern University. Matthew served as Director of CIS and MIS programs at Midstate before joining Bradley University as a lecturer. He obtained his Ph.D. in 2013 and became an assistant professor at Murray State University, specializing in software engineering and computer science education. Matthew is active in community outreach, focusing on K-12 STEM education, and participates in professional activities like journal editing and conference reviewing. He can be contacted at email: mtennyson@murraystate.edu.

Haythem Bany Salameh received his Ph.D. in electrical and computer engineering from the University of Arizona in 2009. Currently a professor of wireless networking at Al Ain University (AAU), UAE, and Yarmouk University, Jordan, also serving as dean of scientific research and graduate studies at AAU. Previously, director of the Queen Rania Center for Jordanian Studies and Community Service, and Director of the Academic Entrepreneurship Center of Excellence at YU. His research interests include optical communication technology and wireless networking, focusing on dynamic spectrum access, radio resource management, and energy-efficient networking. Recipient of prestigious awards for Distinguished Research in the ICT sector and Best Researcher Award at Yarmouk University. Actively serves on the Technical Program Committee of international conferences and as a reviewer for various journals. An IEEE Senior Member since 2016. He can be contacted at email: haythem.banysalameh@aau.ac.ae.