Proceedings of CONF-CDS 2026 Symposium: Data-Centric AI Security: Securing Models, Learning Agents, and Autonomous Systems
DOI: 10.54254/2755-2721/2026.CH33360

Optimization of Privacy Protection Protocols for the Internet of Vehicles (IoV): The Balance Between Communication Performance and Privacy

Yijie Li

Information Technology Department, James Cook University, Singapore, Singapore
yijie.li@my.jcu.edu.au

Abstract. Due to the automotive technology advances, the Internet of Vehicles (IoV) has become a mature field. In China, vehicles primarily connect to the internet through V2X (Vehicle-to-Everything) technology, which supports features like smart cars, autonomous driving, and traffic sharing. However, the high-frequency broadcasting of Basic Safety Messages (BSM) exposes vehicles to significant privacy leaks. Therefore, this paper analyzes the competitive relationship between communication performance and privacy security. To address motion-based linking attacks, this research proposes a mechanism combining Multi-access Edge Computing (MEC) assisted cooperative pseudonym changes. Furthermore, this paper also proposes a mechanism of trajectory perturbation. Finally, the study concludes that this approach reduces the computational burden on vehicles while maintaining high privacy standards through the TPPDP model. The TPPDP model utilizes differential privacy and Laplace noise to balance the performance and privacy of vehicles.

Keywords: IoV, Privacy Protection, MEC, Cooperative Pseudonym Change, Trajectory Perturbation

1. Introduction

Cars provide modern society with immense convenience, but their rapid growth has also created issues like traffic congestion and environmental pollution. The automotive industry is currently moving toward "four new trends": electrification, intelligence, networking, and sharing. These trends require robust communication support provided by the Internet of Vehicles [1]. In many Chinese cities, tests for autonomous and assisted driving have already begun. Even though data interaction improves human happiness and convenience, privacy concerns have become increasingly prominent. Vehicles broadcast Basic Safety Messages (BSM) that contain precise location and identity data, making them vulnerable to tracking attacks. BSM features include high-frequency broadcasting, un-encrypted payloads, and indiscriminate sending modes. Therefore, some attackers can easily use these characteristics to conduct simple linking attacks or syntax linking attacks to identify physical vehicle traits. Plus, the most difficult challenge to solve is the motion prediction attack. Since physical movement is continuous, an attacker can use the speed and direction captured at the moment of a vehicle's ID change to predict the vehicle's next location. However, existing

DOI: 10.54254/2755-2721/2026.CH33360

solutions like group signatures are often too slow for dense traffic. This is because verifying new IDs requires significant computing power. Other methods, such as "silent periods," can cause safety risks by making vehicles temporarily "invisible" to others. This paper explores two methods to balance these communication and privacy needs by using multi-access edge computing to assist RSU and Laplace-based trajectory perturbation.

2. Bottlenecks in existing protocols and privacy schemes

2.1. DSRC and C-V2X technologies

There are two main technical routes for IoV communication. The first is IEEE 802.11p (DSRC), which is suitable for short-range communication but suffers from signal attenuation in dense urban areas. The main reason is that signals are blocked by some buildings. The second route is C-V2X technology, which China actively promotes. This technology uses existing 4G/5G cellular networks to provide wide coverage and high data throughput. Furthermore, C-V2X better meets the requirements for high-level autonomous driving due to its strong signal transmission capability and wide coverage range [2]. Compared to single communication modes such as DSRC, C-V2X adopts a cellular and direct-access converged system architecture first proposed by Professor Chen Shanzhi. This robust PC5 and Uu interfaces architecture enables a variety of communication capabilities. The PC5 interface supports short-range direct communication between time-series devices, providing multi-layered low latency and high reliability for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, which is crucial for real-time applications related to road safety. The Uu interface utilizes existing 4G/5G cellular base station networks to provide telematics services (V2N), which support high-bandwidth data transmission. This dual-interface collaboration mode ensures that C-V2X supports DSRC in terms of communication distance, signal reliability, and pre-control, more effectively supporting future L4/L5 level advanced automatic scheduling requirements [2].

2.2. Limitations of current privacy schemes

Most vehicles currently use Public Key Infrastructure (PKI) to manage pseudonym certificates. However, this approach creates a few specific problems. For Certificate Management aspects, frequent pseudonym changes require the constant update of Certificate Revocation Lists (CRLs). As the number of vehicles grows, the CRL files become massive, which will cause significant validation delays for On-Board Units (OBU). For Signature Complexity, group or ring signatures allow receivers to verify a message without knowing the specific identity of the sender. However, these methods involve bi-linear pairing operations that are extremely time-consuming. Moreover, Roadside Units (RSUs) usually cannot verify hundreds of BSMs within the required safety window at crowded intersections. In ring signatures, all ring members have equal status. Compared to group signature schemes, ring signatures do not have group administrator roles, thus improving vehicle privacy and security. However, ring signature schemes are not as convenient as pseudonym schemes [3]. For Mix-zone Limitations, some schemes use specific physical areas called "mix-zones" to change pseudonyms. Although mix-zones confuse attackers in heavy traffic, the system fails in sparse traffic because attackers can still track the signals effectively.

DOI: 10.54254/2755-2721/2026.CH33360

3. Motion prediction attacks and the core conflict

3.1. Principles of motion prediction attacks

Motion prediction attacks rely on the law of inertia in physical movement. An attacker can use a recursive filter, such as a Kalman Filter to predict vehicles' position in the next time zone. Kalman Filter (KF), also known as a linear quadratic estimation filter, estimates the current states of a system over time recursively using input measurements within a mathematical process model. This algorithm is implemented in two steps: in the prediction step, an estimation of the current state of variables under uncertain conditions is provided. In the next step, after obtaining the measurement, previous estimation is updated by weighted arithmetic mean [4]. Therefore, attackers can use it to estimate a vehicle's future position based on its previous location and speed. As shown in Figure 1, illustration of Kalman Filter-based vehicle state estimation process, the Kalman Filter iteratively refines the vehicle's state estimate by combining the predicted state from the motion model with the new measurement, yielding an optimal state estimate at each time step k. Even if a vehicle changes its ID at a specific time, the attacker can still predict the likely area where that vehicle will appear in the next time zone. This prediction allows the attacker to re-link the new ID to the old one, effectively neutralizing the pseudonym change.

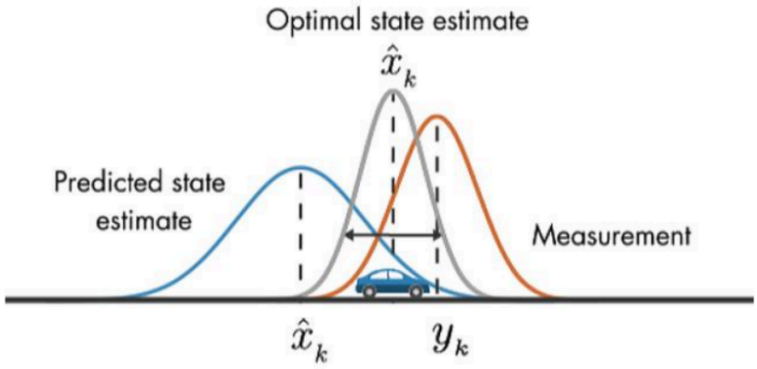

Figure 1. Kalman Filter-based vehicle state estimation process

3.2. The conflict between performance and privacy

Privacy protection in IoV involves two main contradictions: static strategies versus dynamic driving. If a vehicle stops sending BSMs to enter a "silent period" during an ID change, surrounding vehicles may misjudge its position. This lack of communication can lead to serious traffic accidents, such as rear-end collisions. The second contradiction is computational overhead versus latency. Even though complex encryption algorithms provide better privacy, they also increase processing time such as extending verification time. Assisted driving requires a latency of 20 to 100 milliseconds, while fully autonomous driving requires less than 3 milliseconds [5]. If privacy measures exceed these thresholds, they become a threat to safety.

DOI: 10.54254/2755-2721/2026.CH33360

4. Low-latency mechanisms based on edge computing (MEC)

4.1. Multi-access edge computing (MEC)

Multi-access edge computing provides cloud services and computing power at the edge of the network, which is closer to the data source. This platform satisfies the need for agile connections and real-time business processing. Research indicates that MEC can reduce vehicle-to-vehicle latency to under 20 milliseconds [5]. By placing MEC platforms inside base stations, the system can handle certificate verification and lightweight authentication for vehicles. This offloading allows vehicles to react faster to sudden traffic changes while maintaining their privacy.

4.2. Cooperative pseudonym change (CPC)

The Cooperative Pseudonym Change (CPC) mechanism requires RSU and vehicles to work together to change IDs simultaneously. This paper proposes a work flow of how to utilize multi-access edge computing to assist cooperative pseudonym change. First, the Roadside Units (RSUs) continuously monitor the traffic density in their monitoring range and count the number of vehicles. Second, a trigger mechanism is set to execute pseudonym changes and utilize multi-access edge computing for offloading. Then, by leveraging its powerful parallel processing capabilities, the MEC completes batch certificate verification within milliseconds and generates a globally unified synchronized timestamp. After that process, the Roadside Units broadcasts the synchronized change command. All participating vehicles switch to their pre-set new pseudonyms at the precise timestamp via the PC5 interface. Since multiple targets change identifiers simultaneously, attackers face massive trajectory correlation entropy. As a result, attackers cannot predict the exact positions of vehicles. After the pseudonyms change, the MEC issues lightweight Message Authentication Codes (MACs) for the new IDs. In subsequent communications, surrounding vehicles only need to perform simple MAC comparisons. By this action, the need for time-consuming public key verification is eliminated. In this proposed scheme, the RSU monitors the number of vehicles in its area. When the system detects more than five vehicles, the RSU broadcasts a command for all vehicles to change their pseudonym certificates within the same millisecond-level window. Because many vehicles change their identities at once in a tight space, attackers find it nearly impossible to match original trajectories correctly. By utilizing multi-access edge computing to assist RSUs, we can handle a larger number of ID changes in less time. That's how the mechanism balance the privacy and performance.

4.3. Trajectory perturbation strategy with laplace noise &TPPDP algorithms

To enhance the privacy of vehicles in low-traffic areas, this research utilizes the TPPDP model developed by Chen Si and colleagues from the Nanjing University of Science and Technology [6]. TPPDP comprises two sub-algorithms which are TraPro and TraRel. During table processing, the sub-algorithm TraPro handles spatial data using the TI algorithm K-means, with an appropriate K value to classify the data. Its time complexity is O(n^2) and its space complexity is O(n). As for the sub-algorithm TraRel, it has a time complexity and space complexity of O(n). In the table processing, the TraPro algorithm, based on the K-means algorithm's results during initial computation, employs an efficient function for spatial partitioning. For each solution, a utility score is calculated. Let Q be the query function and U be the utility efficiency function [6]. In areas with very low traffic, the CPC mechanism is less effective because there are fewer vehicles to provide confusion. To solve this, this paper proposes a Trajectory Perturbation strategy. This method adds

DOI: 10.54254/2755-2721/2026.CH33360

two-dimensional Laplace noise to the GPS coordinates of the vehicle. The system strictly limits this coordinate offset to 1.5 meters, which is roughly the width of a standard traffic lane. This ensures that the noise does not interfere with collision avoidance systems. To be specific, attackers cannot find the exact positions of vehicles due to the Laplace noise. By utilizing the Laplace noise, the position of vehicles will slightly change to avoid attackers' prediction. The TPPDP model, which incorporates this Laplace noise, has been shown to maintain low latency while meeting differential privacy requirements. Analysis shows that the execution time for the TPPDP algorithm is shorter than competing models like TSTDA or NGTMA.

For Formula 1: The probability density function for the selection of r in the TraPro sub-algorithm is defined as follows [6]:

$$f\left(r\right) = \frac{\exp(\epsilon q(T,r))u(r)}{\int_r \exp\left(\epsilon q(T,r)\right)u(r)dr} \tag{1}$$

For Formula 2: Considering the sensitivity Δq , the ratio of probability densities between neighboring datasets is bounded by [6]:

$$\frac{\exp(\epsilon q(T,r))u(r)}{\int_r \exp\left(\epsilon q(T,r)\right)u(r)dr} \leq \frac{\exp(\epsilon \Delta q)}{\exp(-\epsilon \Delta q)} = \exp\left(2\epsilon \Delta q\right) \tag{2}$$

For Formula 3: In the TPPDP scheme, the total privacy leakage for the sequence of queries is calculated using the chain rule of conditional probability [6]:

$$\frac{Pr(K(T_1)=t)}{Pr(K(T_2)=t)} = \prod_i \frac{Pr[K(T_1)=t_i|t_1,\ldots,t_{i-1}]}{Pr[K(T_2)=t_i|t_1,\ldots,t_{i-1}]} \tag{3}$$

5. Conclusion

To conclude, this papermainly focuses on how to balance vehicles' communication performance and privacy protection. By deeply analyzing the actual obstacles, this paper identifies the disadvantages of current mechanisms and strategies. This paper analyzes the motion prediction attack and takes it as the most serious problem to solve. Additionally, this paper also presents some related background of IoV to help readers understand how it works. Furthermore, this paper mentions two mechanisms: utilizing multi-access edge computing to assist RSUs in implementing cooperative pseudonym changes and adopting a trajectory perturbation strategy with Laplace noise. To balance communication performance and privacy, this paper suggests using MEC to assist cooperative pseudonym changes through RSU. By offloading the authentication load to the edge of the network, the system reduces the pressure on vehicle OBUs. Moreover, cooperative pseudonym change can also enhance the privacy of vehicles due to the ID changing at a same time. Additionally, the TPPDP model uses Laplace noise to make trajectories harder to predict without sacrificing communication speed. By utilizing these two mechanisms, this paper provides a stronger foundation forsecure and efficient vehicular communication.

This research has several limitations that need to be addressed in future work. First is the reliability. Current MEC technology cannot yet guarantee perfectly reliable low-latency communication in all scenarios. Second is the sparse traffic. In very quiet areas, even cooperative changes might not fully hide a vehicle from a determined attacker. Finally, this research should also focus on noise control. The system needs a very precise way to ensure that artificial Laplace noise stays within safe limits in real-world conditions. Future studies will involve simulation experiments

DOI: 10.54254/2755-2721/2026.CH33360

using the SUMO and NS-2 platforms to gather more data on these mechanisms. This research plans to use OpenStreetMap tools to build realistic road models for these simulations. By refining these edge computing and privacy techniques, we can move closer to a future where autonomous driving is both safe and private.

References

[1] Chen, S. (2022) Critical thinking and suggestions on C-V2X with the developments of intelligent connected vehicles. Telecommun. Sci., 38(7): 1–17.
[2] Chen, S., et al. (2020) LTE-V2X IoV Technology, Standards and Applications. People's Posts and Telecommunications Press, Beijing.
[3] Cui, Y., et al. (2019) Privacy Protection of IoV Based on Lattice Ring Signature. J. Comput., 42(5): 1145–1159.
[4] Khodarahmi, M., & Maihami, V. (2023) A review on Kalman filter models. Arch. Comput. Methods Eng., 30(1): 727–747. https: //doi.org/10.1007/s11831-022-09815-7
[5] China Unicom. (2017) China Unicom IoV White Paper. China Unicom, Beijing.
[6] Wu, Y. (2018) Trajectory Privacy Protection Scheme Based on Differential Privacy. Huazhong University of Science and Technology, Wuhan.