SBM-SA: A Safety Beacon Message Separation Algorithm for Privacy Protection in Internet of Vehicles

Zheng Jiang
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Fang-Fang Chua
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Amy Hui-Lan Lim
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Abstract: A safety beacon message (SBM) plays a pivotal role in the Internet of Vehicles (IoV), broadcasting crucial events and road conditions to nearby vehicles. Given the sensitive nature of the data, such as vehicle identity and location, ensuring privacy is paramount. The significance of this research lies in addressing the pressing need for comprehensive privacy protection in the IoV, especially as most existing schemes focus on safeguarding either vehicle identity or location data during exchanges with core servers. The primary objective of this article is to introduce an SBM separation algorithm, termed SBM-SA, designed to holistically protect both identity and location data. Utilising correlation analysis, the SBM-SA stands as an innovative anonymisation privacy algorithm. Through a simulated IoV environment, the accuracy and efficacy of an SBM-SA are meticulously analysed and juxtaposed against prevailing privacy protection schemes. The findings underscore the SBM-SA's potential to significantly enhance privacy measures in the IoV. Implications of this research extend to shaping future privacy protection strategies of the SBM, emphasising the need for holistic and robust solutions in an increasingly interconnected vehicular landscape.

Keywords: Internet of Vehicles (IoV), privacy protection, safety beacon message (SBM).

http://doi.org/10.18080/jtde.v11n4.767

Introduction

With the promotion of the concept of Internet of Things (IoT), the technological evolution and popularity of the IoT are driving the transformation of traditional vehicle self-organising networks in the direction of a connected vehicle network. The development of computing and communication technology as well as a connected vehicle network is expected to provide enormous commercial and research value. Europe commenced the development of intelligent transportation systems (ITS) in the early 1970s and achieved significant advancements in the field of road traffic informatics (RTI). Subsequently, numerous projects were implemented across Europe to expedite the progression of ITS (Lin *et al.*, 2017). In the following decades, ITS has been widely researched and applied, becoming an important research direction and development trend in the field of transportation (Qureshi *et al.*, 2013).

The Internet of Vehicles (IoV) is a network of connected vehicles that can communicate with each other and with external systems, such as traffic management centres, to enhance the safety and efficiency of transportation. IoV safety-related applications comprise collision avoidance systems that leverage sensor data from vehicles to identify possible collisions and notify drivers to take evasive measures. Another safety-related application are emergency response systems, which can automatically call for help and provide location information in the event of an accident. Non-safety-related applications of the IoV include navigation and routing systems, which can help drivers find the most efficient route to their destination, taking into account real-time traffic data. In addition to safety and non-safety applications, there are special types of applications in the IoV called Paid Information Collection (PIC) applications. As the IoV increasingly focuses on using data to provide and optimise services, people are not willing to share their personal or vehicle privacy information. This greatly limits the development of IoV technology. Consequently, IoV service providers are increasingly choosing PIC applications, including crowdsourcing and crowdsensing. The IoV is a typical application of the IoT in ITS, which refers to a network of information exchange between 'people–vehicles–roads–clouds' according to certain communication protocols and data exchange standards. For example, V2V (Vehicle to Vehicle) solves the communication problem between vehicles; V2P (Vehicle to Pedestrian) solves the communication problem between vehicles and pedestrians; V2I (Vehicle to Infrastructure) solves the communication problem between vehicles and roadside infrastructure; and V2N (Vehicle to Network) (vehicle–cloud) (Jeong *et al.*, 2021). These network formats are collectively referred to as V2X (Vehicle to Everything), and their relationships are shown in Figure 1.

http://doi.org/10.18080/jtde.v11n4.767

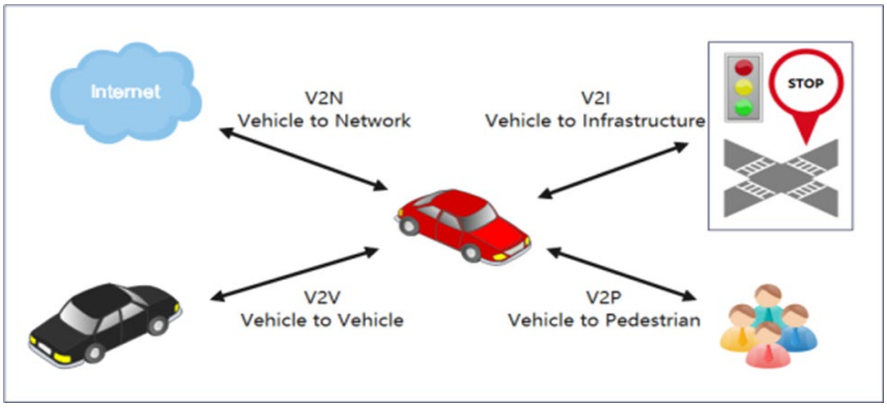

Figure 1. V2X architecture

The architecture of a centralised IoV is depicted in Figure 2, which consists of the core network, certification authority (CA), roadside unit (RSU) and vehicle (Kanumalli *et al.*, 2020). The core network plays an essential role in providing traffic information, services and management functions. The CA is responsible for managing and issuing digital certificates to authenticate vehicles and other devices as legitimate traffic participants. The RSU, installed on the roadside, communicates with vehicles, and provides traffic information and services such as traffic conditions, accident reports and road closure information. The vehicle is the core component of the IoV, communicating with the core network, CA and RSU to receive traffic information and services. The interaction between these components includes the RSU accepting vehicle requests and providing information and services to the vehicle, and the core network accepting vehicle requests and providing information and services to the vehicle. The CA authenticates the vehicle by creating a public key certificate for each vehicle, and the RSU obtains public key certificate information from the CA. Through this interaction, the core network, CA, RSU and vehicle can achieve more intelligent, efficient and secure urban transportation, improving traffic efficiency and safety, and providing a better travel experience for drivers and passengers.

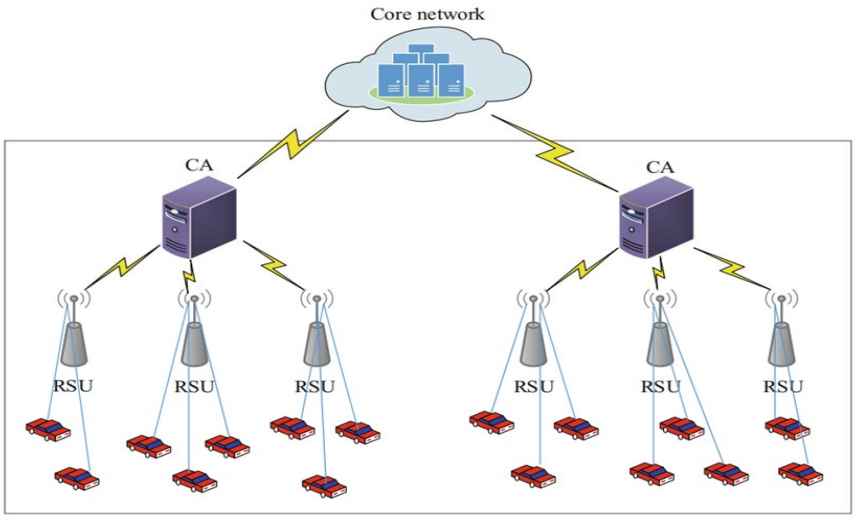

Figure 2. Architecture of a centralised IoV

http://doi.org/10.18080/jtde.v11n4.767

During the V2X interaction, a large amount of message data is transmitted, including an important message type called a safety beacon message (SBM). An SBM is a communication protocol for ITS that aims to improve traffic safety and data exchange rate. It is a short message format used to send specific traffic information to vehicles or other devices. An SBM contains many different types of information, such as road conditions, vehicle driving status, traffic signal status, accident warnings and road closure information. An SBM is transmitted through V2V or V2I communication, allowing driving vehicles to automatically receive and process this information, better adapting to road conditions and improving traffic safety. An SBM is designed to enable different types of vehicles and traffic devices to communicate with each other for improved coordination and management. Standardising and promoting SBMs can help promote the development and application of ITS, improving safety of urban traffic and lower the access threshold of IoV. The SBM uses specific data formats and transmission protocols to ensure timely transmission and correct reception of information. These messages include vehicle position, speed, acceleration, direction and braking statuses. The SBM can also transmit information related to road conditions, traffic flow, accident warnings and other safety-related information. In these messages, identity and location information are particularly important to the IoV. First, identity information is used to identify the legitimacy of participating vehicles in the IoV. Establishing a valid and authorised vehicle identity is essential for maintaining the proper functioning of V2V, facilitating legal responsibility investigation after traffic accidents.

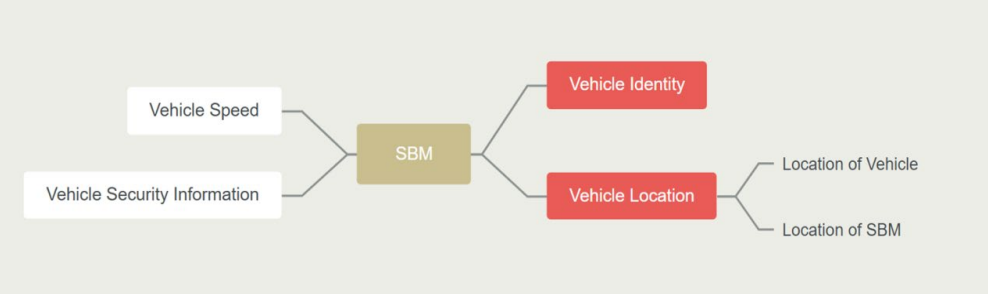

Figure 3. Components of the SBM

As shown in Figure 3, the SBM collected by the vehicle is based on location information and can be divided into two categories: Location of Vehicle (LV) and Location of the SBM (LS). Accurate location information is crucial for V2V to offer high-quality services to users. It is the aggregation and continuous exchange of the SBM that ensures that all connected vehicles can promptly receive safety data and perceive their surrounding traffic environment, including traffic flow, congestion and accidents. At the same time, the SBM can also be integrated with other vehicle communication systems and traffic management centre systems to form a complete traffic management network, make it easier for drivers or other related personnel to understand and use (Li *et al.*, 2018a). SBM is widely used in traffic safety applications in the

http://doi.org/10.18080/jtde.v11n4.767

IoV, including traffic accident warning and avoidance, road traffic information services, and vehicle flow control.

On the other hand, in PIC applications there are privacy leakages before SBM upload. Currently, many scholars have studied privacy protection issues in the IoV and proposed various privacy protection mechanisms based on anonymity, confusion, fuzziness and encryption, etc. However, these privacy protection mechanisms do not consider the correlations of time, space and data factors. Privacy concerns arise in PIC applications, as sharing personal and local sensor data with others is necessary to create useful services and knowledge. For example, the poisson line process algorithm utilises conditional random fields (CRFs) to model the spatiotemporal correlations among group sensing data and proposes an acceleration algorithm to learn the weakness of correlations, thereby enhancing data perception while protecting user privacy through filtering user context (Hou *et al.*, 2022).

The SBM-SA proposed in this paper is an avant-garde algorithm tailored for privacy preservation within the realm of the IoV. This algorithm, underscored by its unique application of correlation analysis, stands in contrast to prevailing methodologies. The SBM-SA is intricately designed to ensure the protection of users' identities and location privacy, all while retaining the comprehensive nature of the data. A salient feature of the SBM-SA is its emphasis on vehicle identity and location during SBM data exchange. Ingeniously, the algorithm clusters vehicles adhering to predefined criteria, leading to the creation of an anonymous group identity (GID). This GID, in essence, acts as a proxy for individual vehicles during the SBM data transmission, fulfilling the overarching privacy mandates. This work delineates a fresh perspective on IoV privacy challenges, setting it apart from previously discussed IoV privacy algorithms.

Literature Review

Privacy protection has gained significant attention in IoV research in recent years (Wu *et al.*, 2020). According to the objectives of privacy protection (PP), it can be divided into three types: PP of identity (Liu *et al.*, 2023), PP of location (Babaghayou *et al.*, 2023) and PP of trajectory (Jegadeesan *et al.*, 2021). Authentication is crucial in protecting the identity privacy of vehicles and receiving data from legitimate vehicles in the IoV. To achieve this, researchers have proposed several authentication mechanisms. For example, fog computing technology is used for pseudonym management in identity authentication, which enhances the ability of identity PP by leveraging the edge computing resources of vehicular networks (Song *et al.*, 2020). Although this solution can partially address the security issues in identity authentication, it is constrained by the computational capability of edge computing resources, leading to performance issues in pseudonym management. Additionally, a decentralised binary

http://doi.org/10.18080/jtde.v11n4.767

lightweight privacy-preserving authentication scheme, called the two-factor lightweight privacy-preserving authentication scheme (2FLIP), has been developed for identity authentication, which reduces authentication costs and achieves conditional privacy protection through a biometric-based binary approach (Nandy *et al.*, 2021). However, the security of 2FLIP relies on the unique system key stored by the CA. Another proposed authentication protocol is the layered pseudonym authentication protocol, which divides pseudonyms into two sub-ranges based on time, primary and secondary pseudonyms, and is beneficial in reducing the burden of the IoV system by communicating with fully trusted institutions and vehicles (Liu *et al.*, 2023).

With the rise of location-based services in the IoV, protecting the privacy of vehicle location has become a major concern for researchers. For example, one approach to protecting location privacy uses the subdivision method (Sadiah *et al.*, 2022). Firstly, an anonymous server generates a region unit that covers at least a certain number of users based on their true locations. To protect users' location privacy, an anonymous server calculates the geometric centre of the region unit as the anonymous location. This allows users to send or request data using the anonymous location instead of their true location. Additionally, the k-anonymity can also be achieved by using the micro-aggregation method (Ye *et al.*, 2023). The anonymous server sends data of k users together to the core server, resulting in confusion for the core server in identifying which data belongs to which user. Therefore, the micro-aggregation method only partially satisfies the requirements of location PP. The collection of vehicle trajectory data can help alleviate the pressure on the traffic management system in areas such as traffic congestion and tracking of offending vehicles. Therefore, research on vehicle trajectory PP has received widespread attention. An example of this data collection is the homomorphic encryption schemes which are used to achieve trajectory PP through key sharing between vehicles (Acar *et al.*, 2018). However, this key-sharing method has limitations and can only be applied in environments with high vehicle density. Another example is the use of a trajectory privacy strategy with multiple mixed regions (Memon *et al.*, 2018). By constantly changing pseudonyms, the pseudonyms cannot be linked, thereby protecting vehicle trajectory privacy. Some researchers have also proposed a route reporting scheme with privacy protection (Zhang *et al.*, 2020b). The proposed scheme employs both homomorphic encryption and error-checking and correction techniques to conceal and combine vehicle trajectories. By doing so, it not only ensures the privacy of drivers' paths but also mitigates collusion attacks from potentially malicious vehicles. In addition, according to the implementation mechanism of privacy protection, it can be divided into three types: PP of anonymity-based, PP of fuzziness-based and PP of encryption-based mechanisms (Garg *et al.*, 2020).

http://doi.org/10.18080/jtde.v11n4.767

The PP of anonymity-based mechanisms aims to protect the privacy of vehicle users by concealing their actual identity or location. To achieve this, k-anonymity technology is often employed, which anonymises the user's identity or location with k-anonymity as the core concept (Wang *et al.*, 2022). The maximum entropy principle is used to identify k suitable vehicles whose historical request probabilities are closest to that of the real vehicle, thereby protecting the privacy of the vehicle's identity or location. However, PP mechanisms based on anonymity typically require a trusted third-party anonymous server (such as a CA). This approach is only suitable for centralised applications, and the anonymous server may become a bottleneck when there are a large number of users, leading to slow service response times and poor user experience. Conversely, when the number of users is small, it may be difficult to achieve k anonymisation in a timely manner, rendering the PP of anonymity-based mechanism ineffective.

PP of fuzzy-based mechanisms often modify data attributes to safeguard user privacy. This involves using fake data for communication to avoid revealing the user's actual information. Random data perturbation techniques, such as adding random noise to the user's actual data, are commonly used. However, the method based on fuzziness results in significant information loss, which seriously affects the quality of service of the vehicular networks. Therefore, in practical vehicular network applications, the PP mechanism based on fuzziness is generally not used to protect user privacy.

The PP mechanism based on encryption is an important means of information protection. The encryption technologies commonly used include group signatures, bilinear mappings, public key infrastructure (PKI) encryption, and elliptic curve encryption; for example, the MixGroup method based on combining the mix-zone and group signature technologies (Hou *et al.*, 2021). The MixGroup method increases opportunities for anonymous exchanges in the group to protect user identity/location privacy. However, the mechanism based on encryption has high performance requirements for the user's terminal device, such as storage and computing capabilities.

With the accelerating evolution of technological revolution and industrial change, the IoV is gradually shifting towards a data-centred model. However, relying solely on naturally uploaded data from users is far from satisfying the data needs of the IoV. Therefore, the current trend in the IoV is towards PICs, such as crowdsourcing (Lin *et al.*, 2020) and crowdsensing (Qian *et al.*, 2021), which are popular low-cost methods for collecting SBM data. Although these are both PIC applications, they address different IoV scenarios: in IoV crowdsourcing applications, vehicles consciously and actively collect SBM data (Li *et al.*, 2020). The IoV backend publishes crowdsourcing tasks, and voluntary vehicles become targeted vehicles to execute the SBM data collection task. Therefore, the crowdsourcing

http://doi.org/10.18080/jtde.v11n4.767

applications of the IoV are targeted towards individual vehicles, without forming a concept of groups between vehicles, and do not have high requirements for vehicle density. However, crowdsensing applications are an extension of crowdsourcing applications, shifting from vehicles taking the initiative to vehicles passively cooperating without awareness. Therefore, in IoV crowdsensing applications, a group concept is formed among vehicles, and the vehicle group passively cooperates to collect SBM data (Mei *et al.*, 2020). The crowdsensing applications in the IoV require a high density of vehicles to participate in the SBM data collection task, which requires a large amount of SBM data collection, and the SBM data should have a certain correlation to each other.

The concept of crowdsourcing has been around for a long time, mainly referring to the practice of companies or enterprises breaking down a task and assigning it to volunteers, who complete the task in a voluntary and self-directed manner (Kietzmann, 2017). Due to its effectiveness and scalability as a business model, crowdsourcing has become a powerful tool for collecting large amounts of data at a relatively low cost, providing a potential solution to the high cost of data collection that has traditionally been a major obstacle. In the crowdsourcing applications of the IoV, connected vehicles use smart devices such as high-definition cameras, traffic recorders, communication devices and other sensors to execute crowdsourcing tasks. In the process of executing crowdsourcing tasks in the IoV, the tasks are first published from the IoV backend (central server). Then vehicles voluntarily receive tasks and become targeted vehicles, actively collecting specific data related to traffic safety, such as road conditions, traffic congestion and accidents.

Researchers have proposed various methods for crowdsourcing applications of the IoV. For example, Wang *et al.* (2020) used crowdsourcing to fill the gap in the ITS where events cannot be captured. By having the driver manually enter basic event information and aggregating it with other existing resources (such as TikTok and Twitter), the complete event is formed. The aggregation process is completed by the CrowdITS processing server. Finally, the CrowdITS processing server pushes events that the driver may be interested in, enhancing the driving experience of the ITS. Misra *et al.* (2014) pointed out that crowdsourcing is widely used to collect data from stakeholders, such as crowdsourcing data to solicit feedback on service quality and real-time information quality. Metlo *et al.* (2019) proposed a method for detecting and identifying specific vehicles based on crowdsourced data. The crowdsourced data comes from location data on vehicles obtained by smartphones. Users can wait for the vehicle they want on different routes, thereby tracking the current location of the vehicle and estimating the time required for the vehicle to reach their location. Zhang *et al.* (2020a) used crowdsourcing to aggregate data from multiple vehicles. Utilising this data, they detected and located potholes on multi-lane roads, improving the accuracy of traffic detection. Ali Sarker *et*

http://doi.org/10.18080/jtde.v11n4.767

al. (2021) first used crowdsourcing to collect sensor data (such as accelerometers and GPSs) from vehicle users' smartphones. Then, through dynamic time warping technology, they automatically processed heterogeneous data such as time deformation, speed and time mismatch, thereby improving the accuracy of road monitoring. Yang *et al.* (2018) used crowdsourcing to track the trajectory data of a large number of vehicles. They used a multi-level strategy and detailed data mining techniques to automatically generate road-based intersection maps.

From the above vehicle network crowdsourcing applications, it could be concluded that crowdsourcing is based on the principle of voluntary and active participation of vehicle users in collecting data related to a specific task. However, the aggregation of data may potentially result in privacy breaches for users. It is only through protecting the privacy of vehicle users that these applications can be more actively involved in crowdsourcing tasks and collecting relevant data. Therefore, privacy protection in vehicle network crowdsourcing applications needs to be further studied in order to promote further development of crowdsourcing applications. The advancement of sensors and mobile devices has led to the emergence of crowdsensing as a significant technology for gathering and transmitting sensing data (Huang *et al.*, 2017; Zappatore *et al.*, 2019). In a crowdsensing system, users utilise handheld devices as sensing units and collaborate through mobile networks such as Wi-Fi, 4G, and 5G to collect sensing data and complete complex social sensing tasks on a large scale. As a result, crowdsensing applications have gained considerable attention in the domain of the IoV (Li *et al.*, 2018a). Figure 4 illustrates the architecture of a typical crowdsensing system. In crowdsensing-based IoV applications, data perception and transmission are achieved through the intelligent terminals of vehicles or vehicle users, to obtain various information required for traffic management in a low-cost, fast and simple way; for example, social media analysis (El Khatib *et al.*, 2019), fine-grained air pollution monitoring (Liu *et al.*, 2016), urban environment monitoring (Nandy *et al.*, 2021), and road traffic data collection, etc. Corresponding measures are then taken based on the content of this information to address potential traffic management issues.

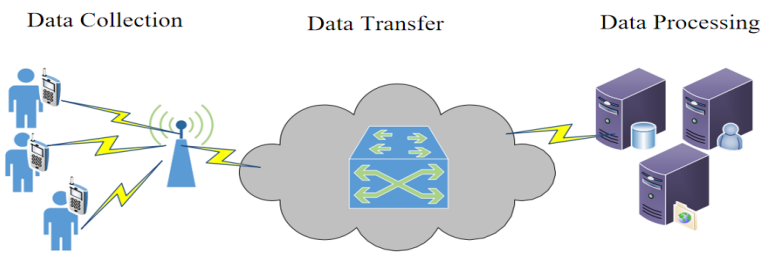

Figure 4. Workflow of crowdsensing system

http://doi.org/10.18080/jtde.v11n4.767

To encourage more users to accept crowdsensing applications, scholars have also studied many incentive mechanisms in crowdsensing systems, such as discrete crowdsensing incentive mechanisms (Liu *et al.*, 2020), trust-based incentive mechanisms based on reverse auctions (Zhang *et al.*, 2022), and offline and online incentive mechanisms for fair task scheduling (Capponi *et al.*, 2019). While incentive mechanisms have boosted users' enthusiasm for crowdsensing and expanded the range of potential applications, more users are now aware of the importance of protecting their personal data and are unwilling to participate in crowdsensing tasks due to privacy concerns. Moreover, the main feature of crowdsensing is the passive involvement of users. Such as users only need to have their smartphones activated, but they may not have complete knowledge of when and what data is being transmitted. The collected sensing data has a large scale and is related to time, space and content. Therefore, the privacy protection of users is worthy of research and discussion concerning crowdsensing applications in the IoV.

Comparison of existing work

In order to determine appropriate proposed methods, it is necessary to collect and compare previous related work. Table 1 summarises the privacy issues in SBM generation due to the inclusion of user location, identity and other information. Many researchers have studied privacy protection in the IoV (Kim *et al.*, 2022; Xiong *et al.*, 2019) and proposed various privacy protection mechanisms, including anonymity-based, obfuscation-based, fuzziness-based and cryptography-based mechanisms. However, these privacy protection mechanisms do not consider the correlation of time, space and data, but simply encrypt or anonymise the data itself. For example, obfuscation-based mechanisms may destroy the semantic information of the data, reduce its comparability, and lead to irreversible obfuscation in the obfuscation process. In the IoV scenario, personal and local sensing data need to be shared with others to generate valuable knowledge and services, which raises concerns about user privacy. Gao *et al.* (2022) proposed a novel trajectory obfuscation algorithm that can effectively hide user location information while maintaining data quality and task completion rates. The algorithm divides the user's trajectory into multiple segments and generates some fake trajectory segments in each segment, which are mixed with the real ones to prevent attackers from determining the user's real location.

However, trajectory obfuscation may affect the accuracy and integrity of data, as fake trajectory segments may introduce noise or interfere with real data. Zhang *et al.* (2021) proposed using geometric range query technology to transform the task recommendation process into finding suitable participants within a geometric range to protect user location privacy. The algorithm first transforms user location information into discrete grid points and

http://doi.org/10.18080/jtde.v11n4.767

then converts the task range into grid point ranges. Next, the algorithm uses geometric range query technology to search for suitable participants within the grid point range, avoiding direct exposure of user location information. The algorithm also uses some privacy protection strategies, such as adding noise to query results and limiting query frequency. However, converting user location and task range into grid points may introduce some discretisation errors, leading to less accurate recommendations. At the same time, geometric range queries require significant computational resources and time, which may affect application performance and response time. An algorithm for task allocation was proposed by Qian *et al.* (2021), which not only optimises task allocation in vehicle-based crowdsensing applications but also ensures PP of location and level of service provided. The algorithm treats participants and tasks in the sensing network as a bipartite graph and uses participants' location privacy and service quality as optimisation objectives and constraints, respectively. The algorithm then uses linear programming techniques to optimise the objective function and constraints to obtain the optimal task allocation algorithm while meeting location privacy and service quality requirements. However, the algorithm only considers location PP and does not consider other types of privacy protection, such as identity and behavioural privacy. At the same time, some researchers have proposed privacy protection strategies for crowdsourcing applications. For example, Zhang *et al.* (2020a) introduced a decentralised spatial crowdsourcing method for location PP in the IoV. This method aims to protect the location privacy of vehicles through decentralisation, while achieving effective spatial crowdsourcing task allocation and data collection. By adopting differential privacy-based data processing techniques, this method ensures that vehicle location information is not leaked, while achieving efficient task allocation and result verification. Liu *et al.* (2022) proposed a privacy protection solution based on data aggregation and batch authentication. By aggregating data, the exposure of individual data is reduced, and batch authentication is used to improve data credibility and processing speed. While protecting data privacy, this method takes into account system processing speed and performance, verifying its effectiveness and feasibility. This solution can be applied to various data-intensive application scenarios, providing a feasible method for privacy protection.

In the rapidly evolving domain of the IoV, a myriad of research has been dedicated to enhancing the privacy of vehicular communications. For instance, Xiong *et al.* (2019) delved into the balance of accuracy and privacy, underscoring the complexities inherent in mobile crowdsensing. While their insights are invaluable, they predominantly cater to specific IoV scenarios, leaving a broader array of challenges unaddressed. On a similar note, Babaghayou *et al.* (2023) and Benarous & Kadri (2022) have made significant strides in location privacy. However, their investigations are largely centred on specific techniques like geometric range

http://doi.org/10.18080/jtde.v11n4.767

queries and obfuscation, respectively. These studies, while groundbreaking in their own right, have yet to offer a comprehensive solution that addresses the multifaceted challenges of IoV privacy in its entirety. The potential of integrating crowdsourcing methodologies with the IoV, as hinted by more recent works like Gao *et al.* (2022) and Hou *et al.* (2021), suggests the possibility of a more encompassing solution. Yet, the literature still yearns for a definitive approach that seamlessly merges these domains.

Table 1. Summary of privacy methods in SBM generation

Source	Description	Method	Limitations
Gao *et al.* 2022	Propose an algorithm for preserving location privacy through obfuscation of trajectories	Differential privacy	➢ The primary focus has been on the protection of location privacy, with an absence of safeguards for other forms of privacy, such as identity and behavioural privacy ➢ Data loss caused by suppressing or obfuscating location data uploads ➢ Algorithms are complex and have performance issues
Zhang *et al.* 2021	Propose the location privacy-preserving task recommendation (PPTR) schemes with geometric range query in mobile crowdsensing without the trusted database owner	Geometric range query	
Qian *et al.* 2021	Use the differential privacy algorithm to preserve location privacy of the vehicle and submit it to IoV applications	Differential privacy	
Zhang *et al.* 2020a	A spatial crowdsourcing method for decentralised location privacy protection based on differential privacy algorithm is proposed for the IoV	Differential privacy	
Liu *et al.* 2022	Propose a privacy-preserving solution for data aggregation and batch authentication using differential privacy algorithm	Differential privacy	

From the synthesis of the literature, it is evident that within the intricate landscape of the IoV, privacy challenges are continuously evolving and diversifying. Concurrently, an escalating urgency exists to protect both the vehicle's location and the owner's identity. Distinct from solutions proposed in existing literature, this paper introduces the SBM-SA, a privacy-centric algorithm. Utilising correlation analysis, the SBM-SA offers a robust dual-layered protection

http://doi.org/10.18080/jtde.v11n4.767

mechanism safeguarding both the vehicle owner's identity and the vehicle's location data, thereby addressing this domain's existing gaps.

SBM-SA Design

In addressing the research gaps mentioned in the earlier sections. In this section, the proposed SBM separation algorithm (SBM-SA) is described. The SBM includes various types of data, and the SBM-SA mainly focuses on three types: road SBM (S1), accident SBM (S2) and traffic flow SBM (S3). Considering the directionality of data transmission, this section mainly analyses the data transmission scenario between vehicles and the core server in the IoV. After generating the SBM, when vehicle users upload the collected SBM to the core server for aggregation, they must also upload the event location (*EL*) of the SBM. This is because knowing the location of the traffic event is necessary to effectively utilise the SBM. For example, in the case of traffic jam, knowing the location of the jam is necessary to guide other vehicles to avoid the road jam segment. Without this location information, the traffic event itself is meaningless. However, the *EL* where the SBM occurred is likely to be the location where the vehicle passed. Therefore, the core server can infer the location where the vehicle appeared by analysing the *EL* in the SBM, which poses a privacy risk in the data generation process. To address this privacy threat, the SBM-SA is proposed. The SBM-SA mainly draws on anonymous privacy algorithms, including k-anonymity and l-diversity. However, anonymous privacy algorithms may lead to data correlation problems, that is, the anonymised data can still be restored or inferred to the original data through other information or multiple queries, thereby reducing the effectiveness of privacy protection. Therefore, the SBM-SA has been optimised for specific scenarios as explained below.

To update the core server with important information such as road maintenance, traffic congestion, traffic light changes, traffic accidents and traffic flow, vehicle U is required to upload the collected SBM. The SBM should also provide the *EL* for accuracy and reliability purposes. If the *EL* of the SBM is not provided, the value of the SBM collected by the vehicle to the IoV will be reduced. Assuming that the collected SBM has been uploaded, the vehicle can infer that it was present at the location where the SBM occurred. Therefore, directly uploading the collected SBM is highly likely to leak the vehicle's *EL*. For example, U is located at location EL_i. Just at this time, there was a car accident at location EL_i. Then, U collected the relevant SBM data Msg (EL_i) and uploaded it to the core server. If location El_i is important to vehicle U, the core server may invade the vehicle's location privacy. Furthermore, regardless of the time and location, if vehicle U sends Msg (EL_i), it can be inferred that vehicle U was present at location EL_i. Therefore, protecting the exact location where the SBM occurred is irrelevant. The purpose of the data upload process is to prevent the core server from obtaining

http://doi.org/10.18080/jtde.v11n4.767

the vehicle's exact location, without considering how to safeguard the location of the SBM occurrence. Therefore, the design purpose of the SBM-SA is to separate the relationship between the vehicle and the core server where an SBM occurs during the data upload process, which helps to safeguard the confidentiality of the vehicle's location information.

The logic and main workflow of the SBM-SA are explained as follows.

The main focus of the SBM-SA is on separation, which ensures the privacy of the vehicle's location by disconnecting the vehicle from the location *EL* where the SBM is collected. To achieve this, when the vehicle (U) collects SBM Msg (*ELO*) at a particular location *ELO*, the SBM-SA employs to separate the vehicle from the location *ELO* where the data was collected.

(1) Vehicle U does not immediately upload the collected SBM data Msg (*ELO*) to the core server. Instead, it first determines the time tolerance of Msg (*ELO*) and selects to upload it to the core server within the time tolerance range T. T is designed based on the corresponding SBM real-time needs to ensure that outdated information is not uploaded.

(2) Instead of uploading the identity of the vehicle, the collected SBM Msg (*ELO*) is uploaded as an anonymous group identity (GID).

(3) The GID not only serves as an identity credential for the uploading vehicle, but also enables data analysis through the correlation between the GID and the SBM, thereby further mining the value of data.

The SBM-SA's goal is to generate vehicle groups and obtain a GID with the help of time tolerance. To achieve this, vehicles passing through location *EL*0 within the time tolerance T are recorded and stored in a vehicle set {V1, V2, V3, ..., Vn}, where n vehicles have passed through *EL*0. The targeted vehicle U is represented by the red vehicle in Figure 5, while all vehicles passing through *EL*0 are represented by the green vehicles. The vehicle group is then initialised as G' = {V1, V2, V3, ..., Vn}. The anonymity degree of vehicle privacy protection is set to p, where a larger anonymity degree indicates better hiding effect of the vehicles. The size of p is determined according to the user's privacy protection requirements. To obtain the final vehicle group G from the initial group G', the final group should include at least p vehicles, and the targeted vehicle U must be included in the final group G to ensure that vehicle U is hidden in group G. In the SBM-SA, if the cardinality of the initial group G' is greater than p (i.e., n >= p), a random selection of p vehicles, which includes vehicle U, is made from G' to update and obtain the final group G = {V1, V2, V3, ..., Vp}. However, if n < p, the SBM-SA needs to select additional p−n vehicles to add to the initial group G'. To do so, a region A is constructed with a centre *ELO* and a radius T, as shown in Figure 5, and the selection of p−n is based on this region. V denotes the average speed of vehicles. According to theoretical analysis, vehicles are unlikely to move beyond region A within time T. In the case where n < p, the SBM-SA will

http://doi.org/10.18080/jtde.v11n4.767

select vehicles in region A that have not yet passed the *ELo*. These vehicles will be merged with the vehicles that have already passed the *ELo* and records them as {V1', V2', V3', ..., Vp–n'}. It is evident that the p–n vehicles are not part of the original set G' of vehicles, as illustrated in Figure 5, where the yellow vehicles represent these p–n vehicles. Subsequently, they are included in the initial set G' to form the final set G and generate a GID for the group G.

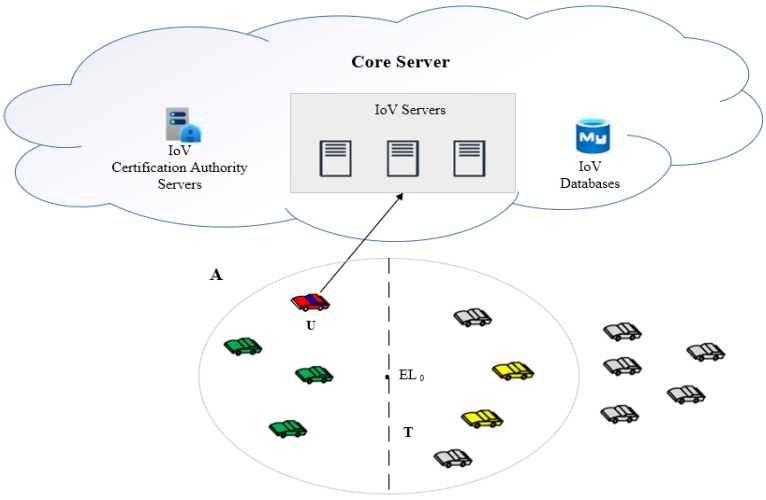

Figure 5. SBM-SA architecture

The generation of a GID can be completed through the above method, and then uploaded to the core server to achieve the goal of separating the connection between vehicles and *ELo* where the SBM occurs, thereby protecting the location privacy of vehicles.

As shown in Algorithm 1, upon collecting SBM data at a location *ELo*, a vehicle waits for a specified time tolerance T before initiating the upload. During this interval, the algorithm tracks all vehicles passing through *ELo*, grouping them into a VehicleSet. If the number of vehicles in this set is less than a desired anonymity degree p, the search expands to a surrounding region A to include more vehicles. Once the set meets the anonymity criteria, a group G is formed, and a GID is generated for it. The SBM data is then uploaded using this GID, ensuring individual vehicle locations remain private. This approach effectively decouples the direct link between a vehicle's exact location and the uploaded data, enhancing location privacy in the IoV context.

Algorithm 1. The pseudo-code of the SBM-SA

Algorithm SBM-SA (SBM data, *ELo*, time tolerance T, anonymity degree p)

Begin

- Wait until time tolerance T before uploading SBM data
- Initialise VehicleSet = vehicles passing through *ELo* within T
- If size of VehicleSet < p then
    - Construct region A centred at *ELo* with radius proportional to T

http://doi.org/10.18080/jtde.v11n4.767

- Add vehicles from region A to VehicleSet until size of VehicleSet = p

End if

- Form group G from VehicleSet ensuring it includes at least p vehicles
- Generate GID for Group G
- Upload SBM data with GID to core server

End algorithm

Data collection for SBM-SA

It is crucial to select the appropriate SBM types that comply with the SBM-SA and utilise them accordingly by filtering out irrelevant ones. Currently, the main sources for obtaining IoV data are open IoV datasets. Two open data sources are considered, namely NGSIM and ApolloScape The NGSIM data set, collected by the US Federal Highway Administration between 2005 and 2010, is a valuable resource for transportation research, including real-world and simulated traffic data from six freeway locations in the United States, with dimensions such as time, location, traffic flow, lane positions, vehicle characteristics and driver behaviour, with a total size of approximately 1.2 terabytes. The ApolloScape dataset was created by Baidu's autonomous driving division, which is a well-known company with map surveying permissions. It includes multiple dimensions for training and testing algorithms for self-driving cars, such as high-definition maps, 3D-point clouds, and camera images. The dataset is currently being maintained and updated by the Apollo team at Baidu. It contains over 100,000 images and high-resolution LiDAR scan data from multiple scenes in multiple cities, and its size depends on the subset used, which may reach several hundred gigabytes or even terabytes.

Selection of simulation platform for the SBM-SA

An IoV simulation environment is a virtual environment used to simulate and evaluate the performance and behaviour of the IoV system. The IoV simulation environment typically encompasses software, hardware and communication networks to mimic diverse IoV application scenarios and traffic situations. The main objectives seek to:

1. Provide simulation scenarios: The IoV simulation environment can provide various traffic scenarios, such as urban traffic, highways, etc., as well as various weather and road conditions to simulate different traffic situations.
2. Simulate vehicle and sensor behaviour: The IoV simulation environment can simulate the behaviour and performance of vehicles and sensors, such as vehicle speed, acceleration, sensor accuracy and response time.

http://doi.org/10.18080/jtde.v11n4.767

3. Evaluate system performance: The IoV simulation environment can simulate the operation and interaction of the IoV system to evaluate its performance and behaviour. For example, it can evaluate communication and collaboration between vehicles and optimise traffic flow and congestion situations.
4. Develop and test IoV applications: The IoV simulation environment can provide an environment for developing and testing IoV applications to verify their functionality and performance.
5. Reduce development and testing costs: The IoV simulation environment can reduce the cost and risk of developing and testing IoV systems and reduce the dependence and impact on the real environment.

Common simulation platforms are presented in Table 2.

Table 2. Summary of privacy methods in SBM generation

Simulation platform	OPNET	CarSim	VIRES VTD
Pros	➢ A relatively complete basic model library is provided ➢ OPNET has a wealth of statistical collection and analysis functions	➢ The simulation results are highly similar to the real vehicle ➢ Co-simulation possible with Simulink	➢ VTD has a rich library of scenes ➢ Synchronously generates OpenDrive high-definition maps
Cons	High cost of learning	Creating a new model takes a long time	Model library is not rich enough
Proposed platform: OPNET is the current mainstream choice, and it has lower requirements on hardware resources, making it more suitable for this research			

OPNET is a commercial network simulation tool that can be used to design, develop and evaluate various networks and systems (Chen *et al.*, 2019). The tool offers a comprehensive range of network models and simulation tools to assess network performance and reliability by emulating different protocols and topologies. To conduct network simulation in OPNET, users need to first define the network topology, nodes and transmission protocols. Users can choose suitable models and components according to their actual needs to build a network system that meets their requirements. OPNET provides users with a variety of tools and analysers that can be used during simulation to assess the performance and reliability of the network system, and to make necessary optimisations. OPNET has rich statistical collection and analysis functions. However, OPNET also has some limitations and challenges, such as a complex configuration and debugging process, which makes the learning curve relatively steep.

http://doi.org/10.18080/jtde.v11n4.767

CarSim is a commercial vehicle simulation software that can simulate various dynamic characteristics and behaviours of vehicles during driving (Wei *et al.*, 2021). CarSim can be used in various application fields, such as vehicle design, control algorithm development, and driver training. CarSim provides multiple vehicle models and control algorithms, which can help users better understand the physical characteristics and behaviour of vehicles during driving. Users can choose suitable models and algorithms according to their actual needs to build a vehicle simulation system that meets their requirements. However, CarSim also has some limitations and challenges, such as the time-consuming process of creating new models, which makes the cost of model creation relatively high.

VIRES VTD (virtual test drive) is a commercial virtual simulation software used for simulating various traffic scenarios and vehicle driving processes (Aoki *et al.*, 2020). It provides a highly customisable virtual environment that helps users better understand the physical characteristics and behaviours of vehicle driving processes. Users can select appropriate vehicle models and control algorithms according to their needs and use various tools and analysers provided by VIRES VTD to evaluate system performance and reliability, and optimise them. VIRES VTD also has some challenges and limitations, such as a relatively small model library, which may limit the range of scenarios that can be tested.

Validation of the SBM-SA

To ensure the accuracy and performance of an SBM-SA, a similar environment must be constructed for validation purposes. Previous studies have suggested several approaches for horizontal comparison, including privacy-preserving schemes based on differential privacy algorithms (Gao *et al.*, 2022; Qian *et al.*, 2021) and geometric range queries (Zhang *et al.*, 2021). These studies can serve as benchmarks for constructing the environment and conducting horizontal comparisons. By using the same environment, the conclusions drawn from these studies can be compared to those of the SBM-SA, thus validating its accuracy and performance.

Application of the SBM-SA

Although the SBM-SA is a privacy protection algorithm specifically designed for the SBM in the IoV, it has broad applications. For example, crowdsourcing and crowdsensing applications in the IoV generate a large amount of SBMs, which is associated with the privacy information of vehicle owners. If this information is not protected, it faces the risk of being misused. Therefore, using the SBM-SA in the IoV is an effective way to protect privacy. The aim of the SBM-SA is to replace vehicle identity with the GID during data upload to separate the

http://doi.org/10.18080/jtde.v11n4.767

association between vehicle identity information and the SBM, thus protecting privacy. Specifically, the steps for designing the SBM-SA in the IoV are as follows:

1. Data collection: First, collecting location and event data of vehicles is essential, such as the location of traffic jams and accident severity, which can be obtained through sensors, in-vehicle radar and other devices.
2. Data preprocessing: Before uploading the SBM, preprocessing work needs to be done, such as removing abnormal data and processing missing values.
3. SBM-SA processing: Through V2I and core server interaction, or through V2V and nearby vehicle interactions, an anonymous vehicle group range is constructed, and key parameters such as anonymity degree p and time tolerance T are obtained. Meanwhile, these core data are passed to the SBM-SA, and the GID is generated through the SBM-SA calculation.
4. Data upload: Use the GID to replace vehicle identity information and upload it with the SBM to the core server for centralised processing.
5. Effect evaluation: Evaluate the data quality and privacy protection effect of SBM-SA processing. Generally, three indicators, anonymity, data availability and data quality, can be used for evaluation.
6. Result application: Apply the SBM-SA processed data to the IoV to protect the privacy information of vehicle owners.

While the SBM-SA effectively decouples the association between vehicle identity and the SBM, it's important to realise that it doesn't offer complete assurance of privacy security and certain risks persist; for example, SBMs still containing sensitive location information. Thus, in real-world applications, further data protection could be accomplished by integrating methods such as differential privacy algorithms. In order to substantiate the efficacy of the SBM-SA in safeguarding the privacy of vehicle owners within the IoV landscape, rigorous testing and validation of the SBM-SA will be conducted and comparative evaluations against other privacy protection algorithms are proposed.

Performance Evaluation

In order to delve deeper into the efficacy and performance of the SBM-SA in terms of privacy protection, this section will undertake rigorous testing and validation of the SBM-SA. We first delineate the details of our simulation environment. Following this, we assess our proposed SBM-SA, contrasting its performance with established privacy protection algorithms such as the PriSC (Zhang *et al.*, 2020a) and the DABAB (Liu *et al.*, 2022). This paper presents a

http://doi.org/10.18080/jtde.v11n4.767

simulation conducted on a PC with an Intel Core i7-7700K @4.0GHz processor and 16GB RAM, leveraging the OPNET simulation software. The simulation creates a vehicle network environment that mirrors a two-way, dual-lane road in accordance with Federal Highway Administration guidelines, with a width of 14.8 metres (four lanes each 3.7 metres wide) and a length of 10 kilometres to replicate a typical 20-minute journey at 30 kilometres per hour. A total of 200 cars are set up to report SBMs, which a designated vehicle collects in three categories: road (S1), accident (S2) and traffic flow (S3), with respective packet sizes of 3,200-bit, 3,400-bit and 3,600-bit. Privacy protection algorithms such as PriSC, DABAB and SBM-SA are implemented during data collection and upload. With a two-second maximum time tolerance for data delay in consideration of user service experience, all three algorithms also maintain a degree of anonymity set at 10. For network communications, the channel spectrum bandwidth is defined at 55 kiloHertz, which affects the data transfer rate and susceptibility to interference. The simulation also employs the Nakagami Channel Model, a flexible tool used to adjust the m parameter, mimicking varying real-world conditions and replicating the fading characteristics of a wireless communication system. Consequently, these parameters (Table 3) significantly shape the simulated network's performance and behaviour.

Table 3. Simulation environment parameter settings

Parameter	Parameter unit	Parameter setting
CPU	X86_64	2 CPU
Storage	TB	1
Road width	metres	3.7 * 4
Road length	km	10
Average vehicle speed	km/h	30
Vehicle transmission power	mW	20
Collected data packet	bit	3,200, 3,400, 3,600
Maximum data transmission rate	Mbps	2
Channel spectrum bandwidth	kHz	55
Channel model	–	Nakagami
Noise power	dBm	-100
Number of cars	–	200

In order to verify the capability of the SBM-SA in protecting the privacy of SBM collection and upload in the IoV, the simulation experiment compares the time delay and privacy leakage probability of PriSC, DABAB, and SBM-SA algorithms in a centralised IoV. Figure 6 shows the time delay of vehicle U collecting different types of SBM through different privacy protection algorithms. When using PriSC and DABAB algorithms to collect the SBM, the data type only causes a minor impact on the delay. However, the PriSC has the largest data delay, approximately 1.6 seconds, while the DABAB performs best at around 0.6 seconds. With the SBM-SA, when the uploaded data is within the permissible time range, different types of SBMs

http://doi.org/10.18080/jtde.v11n4.767

have different time delays. Therefore, in terms of time delay, the SBM-SA does not perform as well as the DABAB.

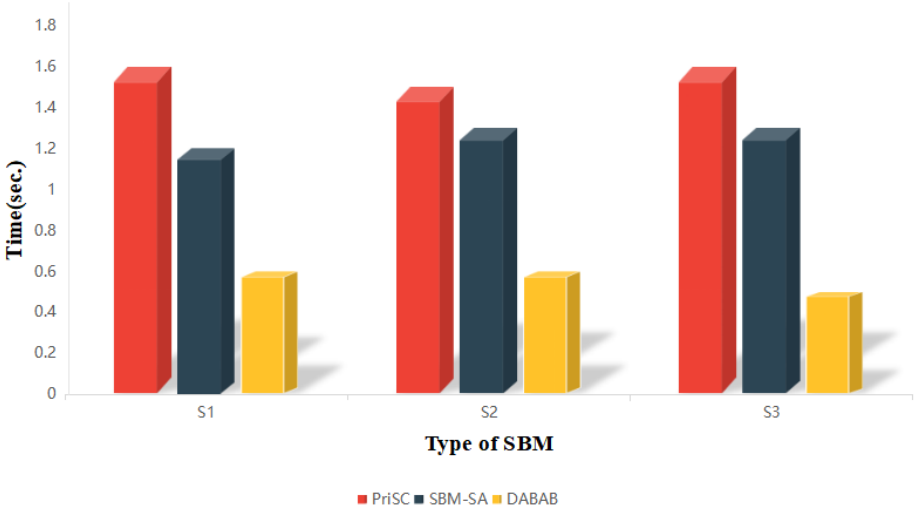

Figure 6. Time delays in the aggregation process of the SBM

The focus of this paper is an experimental exploration of various privacy protection algorithms' efficacy in safeguarding the location privacy of a specific vehicle (U) during its data transmission process. This experimental scenario is set in a context where a core server – functioning as a hypothetical attacker – strives to deduce the location of vehicle U as it uploads data via a message, referred to as Msg (*ELO*), under the effect of different privacy protection algorithms. The core purpose of this investigative setup is to measure how efficiently these diverse algorithms can maintain the vehicle's location privacy throughout the data transfer process. Notably, a successful location guess by the core server equates to a breach of privacy, signifying the respective algorithms' failures in thwarting location exposure. Thus, the experiment provides a comparative evaluation of the tested privacy protection algorithms. Within this experimental setup, certain parameters are accounted for, including the specificities and complexities of the implemented privacy protection algorithms, the volume and variety of data embedded in Msg (*ELO*), and potentially the signal strength or connection conditions during data transmission. While the SBM-SA underperforms the DABAB with regards to time delay, it compensates by delivering superior privacy protection capabilities, albeit at the expense of tolerable time delays, as graphically depicted in Figure 7. With PriSC algorithm, the vehicle U directly uploads the transparent Msg (*ELO*) data to the core server, which then accumulates and processes this data. This direct upload offers the core server a 100% chance of accurately deducing the vehicle's location, implying a complete privacy leak. Conversely, the DABAB, which necessitates an initial data encryption by vehicle U before the upload, decreases the probability of location privacy leakage to between 10% and 20%. Finally, the SBM-SA, being implemented at the user end rather than directly on the core server, poses

http://doi.org/10.18080/jtde.v11n4.767

a greater challenge for the core server in guessing the user's location, consequently reducing the likelihood of privacy leakage for vehicle U to under 10%. Hence, in terms of effective location privacy protection, this paper identifies the SBM-SA as being the most potent algorithm among those tested.

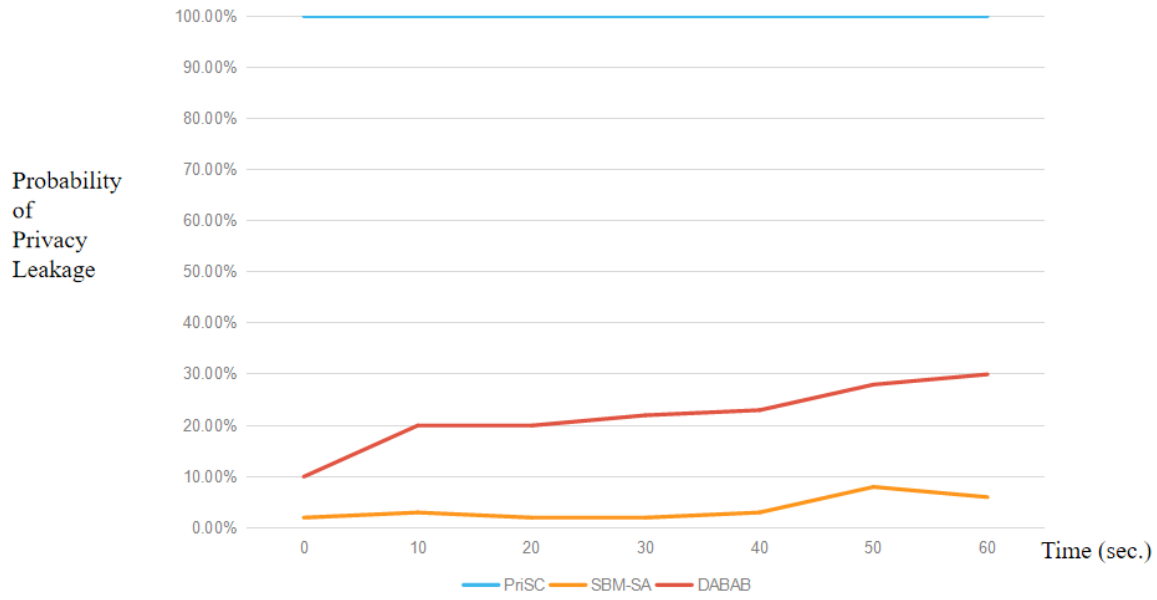

Figure 7. Probability of privacy leakage using different privacy-preserving algorithms during SBM collection

In conclusion, when a series of comparisons are conducted with the PriSC and DABAB algorithms in terms of time and privacy leakage probability, experimental results show that the SBM-SA can effectively protect user location privacy in the IoV.

Conclusion

In the domain of IoV privacy, the SBM-SA has been meticulously evaluated against established algorithms like the PriSC and DABAB. The simulation results derived from the real-vehicle environment simulated by the simulation environment, offer insights into the performance nuances of these algorithms.

The PriSC's architecture is streamlined for swift data transmission, achieved through its direct data upload feature to the core server. However, this expediency compromises privacy, as no encryption or intermediary processing occurs. The DABAB, in contrast, adopts an encryption-first approach. While this ensures data security, the inherent computational demands of encryption introduce latency, evident in the 10% to 20% location privacy leakage. The PriSC's pronounced data delay can be traced back to its simplistic data structure. The absence of protective layers, combined with its direct upload mechanism, renders it vulnerable to location deductions, resulting in a 100% leakage probability. The DABAB, with its layered and

http://doi.org/10.18080/jtde.v11n4.767

encryption-centric design, offers better privacy but at the cost of increased processing time. The encryption process, while bolstering security, adds to the data handling time. The SBM-SA is distinguished by its decentralised data processing, introducing user-end anonymisation. This design choice effectively challenges the core server's location prediction capabilities, reducing privacy leak probabilities to below 10%. The inclusion of the Nakagami Channel Model, simulating real-world wireless communication challenges, further refines the simulation's accuracy. The chosen parameters, especially the 55-kiloHertz channel spectrum bandwidth, play a pivotal role in determining network behaviour. Beyond the surface-level data, the intrinsic design, data structures and processing strategies of these algorithms truly define their efficacy and challenges in IoV privacy.

Discussion

In the realm of IoV privacy protection, the Performance Evaluation section's insights into the SBM-SA's capabilities, especially when juxtaposed with algorithms like the PriSC and DABAB, are enlightening. Grounded in foundational empirical studies, such as those by Zhang *et al.* (2020a) and Liu *et al.* (2022), this research elucidates the nuances and potential of anonymisation of privacy algorithms. The consistent emphasis by prior research on safeguarding user data in today's data-centric era is a testament to the burgeoning interest in this domain. The methodologies adopted in these seminal studies, especially differential privacy, have significantly influenced the trajectory of the SBM-SA. The congruence with prior research not only validates this study's outcomes but also highlights the cumulative wisdom that has shaped this domain. Beyond the immediate results, the broader ramifications beckon attention. The efficacy of the SBM-SA raises pertinent questions about both the IoV's future and ways to amplify privacy protection. While the SBM-SA's success heralds a promising future, inherent limitations delineate ripe scenarios for future exploration and refinement.

Acknowledgements

A version of this paper was presented at the third International Conference on Computer, Information Technology and Intelligent Computing, CITIC 2023, held in Malaysia on 26-28 July 2023.

References

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR), 51*(4), 1–35. https://doi.org/10.1145/3214303

Ali Sarker, M. R., Hassanuzzaman, M., Biswas, P., Dadon, S. H., Imam, T., & Rahman, T. (2021). An efficient surface map creation and tracking using smartphone sensors and crowdsourcing. *Sensors*, *21*(21), 6969. https://doi.org/10.3390/s21216969

Aoki, S., Jan, L. E., Zhao, J., Bhat, A., Rajkumar, R. R., & Chang, C. F. (2020, October). Co-simulation platform for developing inforich energy-efficient connected and automated vehicles. In *2020 IEEE Intelligent Vehicles Symposium (IV)*, 1522–1529. IEEE. https://doi.org/10.1109/IV47402.2020.9304664

Babaghayou, M., Chaib, N., Lagraa, N., Ferrag, M. A., & Maglaras, L. (2023). A safety-aware location privacy-preserving IoV scheme with road congestion-estimation in mobile edge computing. *Sensors*, *23*(1), 531. https://doi.org/10.3390/s23010531

Babaghayou, M., Labraoui, N., Ari, A. A. A., Lagraa, N., & Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications*, *55*, 102618. https://doi.org/10.1016/j.jisa.2020.102618

Benarous, L., & Kadri, B. (2022). Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles. *Peer-to-Peer Networking and Applications*, *15*(1), 461–472. https://doi.org/10.1007/s12083-021-01233-z

Capponi, A., Fiandrino, C., Kantarci, B., Foschini, L., Kliazovich, D., & Bouvry, P. (2019). A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities. *IEEE Communications Surveys & Tutorials*, *21*(3), 2419–2465. https://doi.org/10.1109/COMST.2019.2914030

Chen, M., Miao, Y., Humar, I., Chen, M., Miao, Y., & Humar, I. (2019). Introduction to OPNET network simulation. *OPNET IoT Simulation*, 77–153. https://doi.org/10.1007/978-981-32-9170-6_2

El Khatib, R. F., Zorba, N., & Hassanein, H. S. (2019, December). Crowdsensing-based prompt emergency discovery: A sequential detection approach. In 2019 *IEEE Global Communications Conference (GLOBECOM)*, 1–6. IEEE. https://doi.org/10.1109/GLOBECOM38437.2019.9013852

Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., & Zhang, J. (2022). Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing. *IEEE Transactions on Industrial Informatics*, *18*(9), 6290–6299. https://doi.org/10.1109/TII.2022.3146281

Garg, T., Kagalwalla, N., Churi, P., Pawar, A., & Deshmukh, S. (2020). A survey on security and privacy issues in IoV. *International Journal of Electrical & Computer Engineering, 10(5)*. http://doi.org/10.11591/ijece.v10i5.pp5409-5419

Hou, L., Yao, N., Lu, Z., Zhan, F., & Liu, Z. (2021). Tracking based mix-zone location privacy evaluation in VANET. *IEEE Transactions on Vehicular Technology*, *70*(10), 10957–10969. https://doi.org/10.1109/TVT.2021.3109065

Hou, P., Li, B., Wang, Z., & Ding, H. (2022). Joint hierarchical placement and configuration of edge servers in C-V2X. *Ad Hoc Networks*, *131*, 102842. https://doi.org/10.1016/j.adhoc.2022.102842

Huang, Z., Liu, S., Mao, X., Chen, K., & Li, J. (2017). Insight of the protection for data security under selective opening attacks. *Information Sciences*, *412*, 223–241. https://doi.org/10.1016/j.ins.2017.05.031

Jegadeesan, S., Obaidat, M. S., Vijayakumar, P., & Azees, M. (2021). SEAT: secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management. *IEEE Transactions on Green Communications and Networking, 6*(2), 815–824. https://doi.org/10.1109/TGCN.2021.3126618

Jeong, H. H., Shen, Y. C., Jeong, J. P., & Oh, T. T. (2021). A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. *Vehicular Communications*, *31*, 100349. https://doi.org/10.1016/j.vehcom.2021.100349

Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. *International Journal of Advanced Computer Science and Applications*, *11*(1). https://doi.org/10.14569/ijacsa.2020.0110157

Kietzmann, J. H. (2017). Crowdsourcing: A revised definition and introduction to new research. *Business horizons, 60(2), 151–153*. https://doi.org/10.1016/j.bushor.2016.10.001

Kim, J. W., Edemacu, K., & Jang, B. (2022). Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. *Journal of Network and Computer Applications, 200*, 103315. https://doi.org/10.1016/j.jnca.2021.103315

Li, H., Pei, L., Liao, D., Zhang, M., Xu, D., & Wang, X. (2020). Achieving privacy protection for crowdsourcing application in edge-assistant vehicular networking. *Telecommunication Systems*, *75*, 1–14. https://doi.org/10.1007/s11235-020-00666-w

Li, H., Liao, D., Sun, G., Zhang, M., Xu, D., & Han, Z. (2018a). Two-stage privacy-preserving mechanism for a crowdsensing-based VSN. *IEEE Access*, *6*, 40682–40695. https://doi.org/10.1109/ACCESS.2018.2854236

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018b). Significant permission identification for machine-learning-based android malware detection. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219

Lin, Y., Wang, P., & Ma, M. (2017, May). Intelligent transportation system (ITS): Concept, challenge and opportunity. In 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS), (pp. 167-172). IEEE. https://doi.org/10.1109/BigDataSecurity.2017.50

Lin, H., Garg, S., Hu, J., Kaddoum, G., Peng, M., & Hossain, M. S. (2020). Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *22*(6), 3755–3764. https://doi.org/10.1109/TITS.2020.3025247

Liu, Y., Wang, H., Peng, M., Guan, J., & Wang, Y. (2020). An incentive mechanism for privacy-preserving crowdsensing via deep reinforcement learning. *IEEE Internet of Things Journal*, *8*(10), 8616–8631. https://doi.org/10.1109/JIOT.2020.3047105

Liu, J., Peng, C., Sun, R., Liu, L., Zhang, N., Dustdar, S., & Leung, V. C. (2023). CPAHP: Conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV. *IEEE Transactions on Vehicular Technology*, *72*(7), 8929–8940. https://doi.org/10.1109/TVT.2023.3246466

Liu, K., Li, H., Chen, X., Liao, D., Peng, L., & Yurui, L. (2022, October). A privacy protection solution based on data aggregation and batch authentication. In Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, 85–90. https://doi.org/10.1145/3555661.3560869

Liu, T., Zhu, Y., Yang, Y., & Ye, F. (2016, December). Incentive design for air pollution monitoring based on compressive crowdsensing. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE. https://doi.org/10.1109/GLOCOM.2016.7841892

Mei, Q., Gül, M., & Shirzad-Ghaleroudkhani, N. (2020). Towards smart cities: Crowdsensing-based monitoring of transportation infrastructure using in-traffic vehicles. *Journal of Civil Structural Health Monitoring*, *10*(4), 653–665. https://doi.org/10.1007/s13349-020-00411-6

Memon, I., Chen, L., Arain, Q. A., Memon, H., & Chen, G. (2018). Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. *International Journal of Communication Systems*, *31*(1), e3437. https://doi.org/10.1002/dac.3437

Metlo, S., Memon, M. G., Shaikh, F. K., Teevno, M. A., & Talpur, A. (2019). Crowdsource based vehicle tracking system. *Wireless Personal Communications*, *106*(4), 2387–2405. https://doi.org/10.1007/s11277-019-06323-z

Misra, A., Gooze, A., Watkins, K., Asad, M., & Le Dantec, C. A. (2014). Crowdsourcing and its application to transportation data collection and management. *Transportation Research Record*, *2414*(1), 1–8. https://doi.org/10.3141/2414-01

Nandy, T., Idris, M. Y. I., Noor, R. M., Wahab, A. W. A., Bhattacharyya, S., Kolandaisamy, R., & Yahuza, M. (2021). A secure, privacy-preserving, and lightweight Authentication scheme for VANETs. *IEEE Sensors Journal*, *21*(18), 20998–21011. https://doi.org/10.1109/JSEN.2021.3097172

Qian, Y., Ma, Y., Chen, J., Wu, D., Tian, D., & Hwang, K. (2021). Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks. *IEEE Transactions on Intelligent Transportation Systems, 22*(7), 4367–4375. https://doi.org/10.1109/TITS.2021.3086837

Qureshi, K., & Abdullah, H. (2013). A survey on intelligent transportation systems. *Middle East Journal of Scientific Research*, *15*, 629–642. https://doi.org/10.5829/idosi.mejsr.2013.15.5.11215

Sadiah, S., & Nakanishi, T. (2022). An efficient anonymous reputation system for crowdsensing. *Journal of Information Processing*, *30*, 694–705. https://doi.org/10.2197/ipsjjip.30.694

Song, L., Sun, G., Yu, H., Du, X., & Guizani, M. (2020). Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE*

Transactions on Vehicular Technology, *69*(5), 5403–5415. https://doi.org/10.1109/TVT.2020.2977829

Wang, T., Xu, L., Zhang, M., Zhang, H., & Zhang, G. (2022). A new privacy protection approach based on k-anonymity for location-based cloud services. *Journal of Circuits, Systems and Computers*, *31*(05), 2250083. https://doi.org/10.1142/S0218126622500839

Wang, D., Huang, C., Shen, X., & Xiong, N. (2020). A general location-authentication based secure participant recruitment scheme for vehicular crowdsensing. *Computer Networks*, *171*, 107152. https://doi.org/10.1016/j.comnet.2020.107152

Wang, X., Zhang, J., Tian, X., Gan, X., Guan, Y., & Wang, X. (2017). Crowdsensing-based consensus incident report for road traffic acquisition. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2536–2547. https://doi.org/10.1109/TITS.2017.2750169

Wei, H., Wang, J., Jian, M., Mei, S., & Huang, M. (2021, April). Steer-by-Wire Control System Based on Carsim and Simulink. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–5. IEEE. https://doi.org/10.1109/IEMTRONICS52119.2021.9422502

Wu, Z., Wang, R., Li, Q., Lian, X., Xu, G., Chen, E., & Liu, X. (2020). A location privacy-preserving system based on query range cover-up or location-based services. *IEEE Transactions on Vehicular Technology*, *69*(5), 5244–5254. https://doi.org/10.1109/TVT.2020.2981633

Xiong, J., Ma, R., Chen, L., Tian, Y., Li, Q., Liu, X., & Yao, Z. (2019). A personalized privacy protection framework for mobile crowdsensing in IIoT. *IEEE Transactions on Industrial Informatics*, *16*(6), 4231–4241. https://doi.org/10.1109/TII.2019.2948068

Yang, X., Tang, L., Niu, L., Zhang, X., & Li, Q. (2018). Generating lane-based intersection maps from crowdsourcing big trace data. *Transportation Research Part C: Emerging Technologies, 89*, 168–187. https://doi.org/10.1016/j.trc.2018.02.007

Ye, X., Zhu, Y., Zhang, M., & Deng, H. (2023). Differential privacy data release scheme using micro-aggregation with conditional feature selection. *IEEE Internet of Things Journal, 10*(20), 18302–18314. https://doi.org/10.1109/JIOT.2023.3279440

Zappatore, M., Loglisci, C., Longo, A., Bochicchio, M. A., Vaira, L., & Malerba, D. (2019). Trustworthiness of context-aware urban pollution data in mobile crowd sensing. *IEEE Access*, *7*, 154141–154156. https://doi.org/10.1109/ACCESS.2019.2948757

Zhang, J., Yang, F., Ma, Z., Wang, Z., Liu, X., & Ma, J. (2020a). A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *22*(4), 2299–2313. https://doi.org/10.1109/TITS.2020.3010288

Zhang, C., Zhu, L., Ni, J., Huang, C., & Shen, X. (2020b). Verifiable and privacy-preserving traffic flow statistics for advanced traffic management systems. *IEEE Transactions on Vehicular Technology, 69(9), 10336–10347.* https://doi.org/10.1109/TVT.2020.3005363

Zhang, C., Zhu, L., Xu, C., Ni, J., Huang, C., & Shen, X. (2021). Location privacy-preserving task recommendation with geometric range query in mobile crowdsensing. *IEEE*

Transactions on Mobile Computing, 21(12), 4410–4425. https://doi.org/10.1109/TMC.2021.3080714

Zhang, G., Hou, F., Gao, L., Yang, G., & Cai, L. X. (2022). Nondeterministic-mobility-based incentive mechanism for efficient data collection in crowdsensing. *IEEE Internet of Things Journal*, *9*(23), 23626–23638. https://doi.org/10.1109/JIOT.2022.3190565