Discussion on the Management of spatio-temporal Data Security for Intelligent Connected Vehicles

Yingchen LI [1], Huidong ZOU [1], Qian LIAO [2], Huixian Chen [1], Long HUANG [1], Lei SHI [1],Jinghui BAI [1]

[1]Natural Resources Department Map Technology Review Center, People's Republic of China
[2] Sinomaps press

Keywords: Intelligent connected vehicles, data securiy management, geographical information security, sensor

Abstract

The spatio-temporal data of intelligent and connected vehicles (ICVs) represent crucial surveying and mapping data generated by these vehicles. The massive collection, processing, and aggregation of such data pose potential security risks to geographic information security and even national security. This paper analyzes the significance of spatio-temporal data in ICVs and provides extensive application examples. By comparing the current research status in the United States, the European Union, Japan, it elaborates in detail on China's management status and summarizes practical experience in multiple advanced cities within the country for safety management.Incorporating the current domestic processes of spatio-temporal data generation, transmission, and processing, the paper assesses data security risk,network security risk, and system security risk. Furthermore, this paper proposes recommendations on how to establish spatio-temporal data security management system from various levels, including government, enterprises, and society, to effectively address potential and existing security risks.

1. Introduction

Intelligent Connected Vehicles(ICVs) are installed or integrated with satellite navigation positioning modules, inertial measurement units, cameras, Light Detection and Ranging (LiDAR), and other sensors. The behavior of collecting, storing, transmitting, and processing geospatial information data such as spatial coordinates, images, point clouds, and their attribute information of vehicles and surrounding road facilities during operation, service, and road testing is considered surveying and mapping activities as stipulated by the 《Surveying and Mapping Law of the People's Republic of China》.The ICV industry is rapidly developing in recent years, and the spatio-temporal data collected by its sensors is diverse, highly accurate, and large-scale. The data includes geographic information positions and images, attribute class information of national security departments, posing risks and hidden dangers to the security of geographic information during collection, transmission, storage, and usage.Therefore, the security management of spatio-temporal data for intelligent connected vehicles has become a major issue that urgently needs to be addressed. This paper analyzes the practices of the the United States, European Union, and others in the field of data security for intelligent connected vehicles. It combines domestic policies and regulations on data security and data elements to conduct research and proposes a discussion on the current state of security management for spatio-temporal data of ICVs.

2. Features of spatio-temporal data of intelligent and connected vehicles

2.1 Basic definition

ICV is an automobile equipped with capabilities for environmental perception, intelligent decision-making, and automatic control, as well as the ability to interact with and even collaboratively control external information sources.

Spatio-temporal data of ICV refer to the geographic information data generated by these vehicles, which possess temporal and spatial characteristics.

2.2 Applications of Spatio-Temporal Data in Intelligent and Connected Vehicles

ICVs are equipped with advanced on-board sensors, controllers, actuators, and other devices, which integrate modern communication and networking technologies to enable intelligent information exchange and sharing between vehicles, people, roads, and back-end systems, thereby achieving safe, comfortable, energy-efficient, and high-performance driving. These vehicles, armed with devices such as LiDAR, millimeter-wave radars, optical cameras, GNSS system, and inertial navigation units, can collect vast amounts of data including vehicle data, exterior geographic information, and personal information. However, the potential for data breaches resulting from cyber attacks on such data poses significant risks to national and public security.

In recent years, the rapid technological advancements in the field of ICV have made the risks and challenges facing spatio-temporal data increasingly prominent. In response, national and local governments have issued policies, regulations, and technical guidelines to guide the orderly and healthy development of security supervision for spatio-temporal data in intelligent and connected vehicles.

This article primarily focuses on analyzing the security management of spatio-temporal data in intelligent and connected vehicles. It examines the measures required to protect this critical data from unauthorized access, theft, manipulation, or destruction, ensuring the confidentiality, integrity, and availability of the information collected and processed by these vehicles. The analysis encompasses strategies for implementing robust cybersecurity measures, enhancing data encryption and privacy protection, and complying with relevant regulations and standards to mitigate potential threats and safeguard national and public safety.

2.3 The Importance of Spatio-Temporal Data in Intelligent and Connected Vehicles

Spatio-temporal data in ICVs encompass a wide range of information, including location data, point cloud data, image data, inertial navigation data, and attribute information related

This contribution has been peer-reviewed.
https://doi.org/10.5194/isprs-archives-XLVIII-3-2024-301-2024 | © Author(s) 2024. CC BY 4.0 License.

to vehicles and their surrounding road infrastructure. High-precision location trajectories and positioning data are crucial for realizing autonomous driving. Vehicles can also record precise location information along their travel routes and the surrounding environment, which serves as the foundation for precise navigation and positioning. Point cloud data, acquired through sensors such as LiDAR, generate high-resolution three-dimensional point cloud maps of the vehicle's surroundings. These point clouds not only contain positional information about the environment but also geometric features like the shape and size of objects, providing a detailed environmental model for intelligent and connected vehicles.

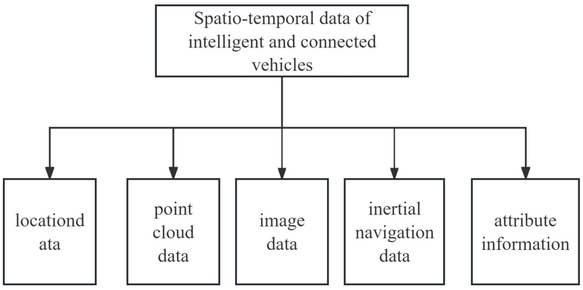

Figure1. The content of spatio-temporal data in intelligent and connected vehicles

Inertial navigation data provides real-time information on a vehicle's acceleration, angular velocity, and attitude, which forms the basis for accurate positioning and attitude estimation. The spatio-temporal data contains rich semantic information. When large amounts of such data from multiple vehicles are aggregated and processed, a lack of standardized collection and effective supervision can lead to unpredictable issues related to geographic information security, particularly concerning is the potential involvement of sensitive geographic information, such as military management areas. Illegal collection or leakage of such data can pose significant risks to social security and even national geographic information security.

3. Research progress of space-time data of intelligent connected vehicles at home and abroad

In general, in recent years, China's research on the management of spatio-temporal data security for intelligent and connected vehicles has focused on the risks in this regard. In comparison, there is less research in this field abroad, according to the publicly available information.

3.1 The United States

In 2017, the United States House of Representatives proposed the "Self Drive Act," aimed at strengthening cybersecurity oversight for connected vehicles.In 2020, the United States released "Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0," which outlined ten technical principles, one of which is ensuring privacy and data security.

3.2 Germany

In 2017, Germany officially released the *Road Traffic Act (Eighth Amendment)* requiring autonomous vehicles to store time and location data when the autonomous driving system is in control, and that the stored data should generally be deleted after six months. In March 2021, Germany passed the *Automated Driving Act*, allowing vehicles to use Level 4 autonomous driving functions in specific application scenarios. Vehicle owners are obligated to save the following data: vehicle identification number; location data; system monitoring data; environmental and weather conditions; network parameters (including transmission delays, etc.); the names of activated and deactivated passive and active safety systems; instances where the safety system was triggered, etc.

3.3 European Union

In 2019, the European Union issued the *EU Guidelines on the Process for Granting Exemptions from Type-Approval Requirements for Automated Vehicles*, which focuses on Level 3 and Level 4 autonomous vehicles and aims to coordinate the temporary safety assessment activities of autonomous vehicles among member states. The *General Data Protection Regulation* (GDPR) of the European Union has direct binding force on autonomous vehicle products within the EU.

3.4 Japan

In September 2018, Japan's Ministry of Land, Infrastructure, Transport, and Tourism formulated and released the *Guidelines for Safety Technologies of Automated Vehicles*, which put forward clear requirements for data recording and cybersecurity. In 2019, the Japanese Cabinet issued an amendment to the *Road Transport Vehicle Act*.

3.5 In China

The spatio-temporal data of intelligent connected vehicles falls within the scope of geoinformation security, and the competent authority is the Ministry of Natural Resources of the People's Republic of China. In recent years, the Ministry of Natural Resources has issued a series of policies and measures to safeguard surveying and mapping geoinformation security and promote the development of intelligent connected vehicles.

In 2022, the *Notice on Promoting the Development of Intelligent Connected Vehicles and Safeguarding Surveying and Mapping Geoinformation Security* was issued, which put forward clear requirements for surveying and mapping activities, surveying and mapping actors, relevant qualifications, foreign-invested enterprises, and external transmission.

In 2024, the *Notice on Strengthening the Management of Surveying and Mapping Geoinformation Security Related to Intelligent Connected Vehicles* was released, further strengthening the management of surveying and mapping activities for intelligent connected vehicles. It strictly reviews navigation electronic maps, strengthens the supervision of geoinformation security, encourages exploration of geoinformation security applications, and supports relevant units in researching technical routes such as crowdsourced data collection and real-time updates. In the same year, the Ministry of Natural Resources published two mandatory national standards for public consultation, namely the *Basic Requirements for Safe Processing of Spatio-Temporal Data in Intelligent Connected Vehicles (Draft for Comment)* and the *Basic Requirements for Safety of Spatio-Temporal Data Sensing Systems in Intelligent Connected Vehicles (Draft for Comment).*

In July 2024, five departments, including the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of Natural Resources, the Ministry of

Housing and Urban-Rural Development, and the Ministry of Transport, jointly announced the list of pilot cities for the integrated vehicle-road-cloud" application of intelligent connected vehicles, further advancing the development of China's intelligent connected vehicle industry and technology.

The series of policies and measures issued by China aim to promote technological upgrading and innovation while ensuring national geoinformation security, thereby fostering the healthy development of the intelligent connected vehicle industry.

4. Practice of Intelligent Connected Vehicles in China

To promote the high-quality development of the autonomous driving industry, various regions in China have introduced relevant laws and regulations on autonomous driving. Beijing has publicly released the *Regulations on Autonomous Vehicles in Beijing (Draft for Consultation),* which includes separate provisions on autonomous driving maps and surveying and mapping security, and clearly stipulates requirements for the collection, storage, transmission, and processing of geographic information data to ensure the security of such data. Shanghai has issued the *Regulations of Pudong New Area, Shanghai Municipality on Promoting Innovative Applications of Driverless Intelligent Connected Vehicles,* requiring the ensuring of high-precision map data security. Hangzhou has released the *Notice of the General Office of the Hangzhou Municipal People's Government on the Issuance of the Administrative Measures for the Testing and Application of Intelligent Connected Vehicles in Hangzhou*, clarifying the implementation of map management requirements and strengthening the construction of network and data security capabilities. Wuhan has announced the *Announcement on the Modification Opinions of the Draft Regulations on the Promotion of the Development of Intelligent Connected Vehicles in Wuhan*, exploring the safe application of high-precision maps, crowdsourced data collection and updates, and high-precision location navigation.

The Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Housing and Urban-Rural Development, Ministry of Transport, and other departments have issued the *Notice on Carrying Out the Pilot Work of Access and Road Access for Intelligent Connected Vehicles*, selecting nine consortia, including Chongqing Changan Automobile Co. Ltd., BYD Auto Industry Co. Ltd., to conduct pilot projects for the access and road access of intelligent connected vehicles in seven cities, including Beijing, Shanghai, and Guangzhou. These projects will systematically carry out product testing and safety assessments, exploring and improving the production access management and road traffic safety management system for intelligent connected vehicles.

5. Risk Assessment of spatio-temporal Data Security for Intelligent Connected Vehicles

5.1 Data Security Risk

Intelligent connected vehicles collect spatio-temporal data through various onboard devices such as LiDAR, millimeter-wave radars, optical cameras, Beidou positioning systems, and inertial navigation units. If these data are illegally obtained or misused, they pose serious security risks.

Privacy Leakage: The vehicle's driving data, including location information and driving trajectories, can be leaked to criminals and used for illegal tracking, harassment, or other criminal activities.

National Security Risks: spatio-temporal data may contain sensitive geographic information, such as the locations of military facilities and critical infrastructure. If accessed by hostile forces, this information could pose a severe threat to national security. Vehicles' continuous data collection capabilities mean that a large amount of location and trajectory data, when aggregated, can generate data that involves national secrets, posing a direct threat to national security.

5.2 Network Risk

The transmission of spatio-temporal data in intelligent connected vehicles relies on modern communication and networking technologies, such as Vehicle-to-Everything (V2X) communications, including vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-cloud, and vehicle-to-pedestrian. During communication, it is essential to ensure the confidentiality, integrity, availability, and authenticity of the spatio-temporal data. Therefore, attackers can impersonate legitimate participants in V2X communications by using fake base stations, identity forgery, or dynamic hijacking to intercept communication information. If vehicle communication information is not encrypted or the encryption strength is insufficient, key information is exposed, or all vehicle models use the same symmetric key for V2X communication, it becomes vulnerable to attacks, resulting in the leakage, unauthorized modification, and destruction of communication information.

5.3 System Security Risk

The long lifecycle and complex operating systems of spatio-temporal data in intelligent connected vehicles, along with their high degree of integration, make them prone to vulnerabilities that attackers can exploit to launch malicious attacks. The decision-making mechanisms of intelligent connected vehicles are increasingly dominated by software and algorithms, whose accuracy and security are crucial to the safe operation of the vehicles. If algorithms contain defects or are maliciously tampered with, it could lead to deviations in vehicle decision-making, resulting in unpredictable risks.

6. Establishment of a spatio-temporal Data Security Management System for Intelligent Connected Vehicles

As the value of data elements continues to gain recognition, data security risks have also emerged. As a critical aspect of overall vehicle data security, the spatio-temporal data security of intelligent connected vehicles is receiving heightened attention from governments, enterprises, and universities alike, in their efforts to strengthen the management system. However, given the rapid evolution of spatio-temporal data security management models, the following recommendations are proposed:

6.1 Accelerated Policy Research at the Local Government Level

China's autonomous driving industry is relatively concentrated, with significant regional disparities. Additionally, the rapid technological advancements in the field of spatio-temporal data for intelligent connected vehicles mean that formulating policies and regulations at the ministerial level, which involves extensive research across various regions, often takes a long time. While the Ministry of Natural Resources has issued mandatory national standards for the secure handling of spatio-temporal data and sensors, these standards were initiated early and have a long development cycle, making it difficult to fully consider the current state of new technologies. Therefore, local governments should leverage their strengths in high-precision map pilots, vehicle-road-cloud integration, and other initiatives to expedite research on algorithms, road testing facilities, advanced sensors, and other technical challenges. Tailored policies should be formulated to support the upgrading and development of the industry.

6.2 Enhanced Research on spatio-temporal Data Security Prevention and Control at the Enterprise Level

Automotive companies and map providers should establish comprehensive management systems and technical safeguards for spatio-temporal data security, ensuring that the collection, storage, transmission, and processing of this data comply with relevant laws and regulations. Efforts should be made to strengthen research, development, and application of cybersecurity protection technologies and measures, enhancing the resilience of intelligent connected vehicles' spatio-temporal data throughout its lifecycle against attacks. Strict supplier access and evaluation mechanisms should be implemented to ensure a secure and reliable supply chain. Actively participating in the formulation and promotion of international and domestic standards for spatio-temporal data security in intelligent connected vehicles can help drive the formation of unified industry standards and standardized development.

6.3 Strengthened Data Security Awareness at the Societal Level

Raising awareness requires multi-stakeholder collaboration. Automotive companies should incorporate content on spatio-temporal data security into the smart connected vehicle safety manuals provided to users, guiding them to consciously turn off sensor equipment in military or classified locations and educating them on data security protection. During National Security Education Day events, the content of data security protection for intelligent connected vehicles should be prominently promoted, raising public awareness of security measures.

References

Cui M.,Huang H,Xu Q.,Wang J., Takaaki SEKIGUCHI2,Geng L.,Li K., 2022:Survey of Intelligent and Connected vehicle technologies: Architectures, functions and applications. Journal of Tsinghua University (Science and Technology), 6

Guidance on the Construction of the National Industrial Standard System for the Internet of Vehicles (Intelligent and Connected Vehicles).

J.Jeong,Y. Cho,A. Kim.2020:HDMI-Loc:Exploiting High Definition Map Image for Precise Localization via Bitwise Particle Filter.IEEE Rob. Autom. Lett.,5 (4), pp.6310-6317.

Cai H, Hu Z, Huang G, Zhu D, Su X.2018:Integration of GPS, Monocular Vision, and High Definition (HD) Map for Accurate Vehicle Localization. Sensors.18(10),3270

Heiko, G, Seif, Xiaolong, & Hu. 2016:Autonomous Driving in the iCity—HD Maps as a Key Challenge of the Automotive Industry.Engineering, 2 (2), pp. 159-162.

Lanyi H,Zhiyong S,Huaiguang W,2023:A Localization and Mapping Algorithm Based on Improved LVI-SAM for Vehicles in Field Environments.Sensors (Basel, Switzerland),23(7).

Xu Q., Cai M., Li K., Xu B.,Wang J.,Wu X..2021:Coordinated f ormation control for intelligent and connected vehicles in multip le traffic scenarios. IET Intelligent Transport Systems, 15(1).15 9-173.

Qiu B.,Li G.,2022:Research on Data Security Management of In telligent Connected Vehicle.Chinese Journal of Automotive Eng ineering,12(3):307-313.

Yang M.,Jiang K., Wijaya B.,Wen T.,Miao J.,Huang J., Zhong C.,Zhang W.,Chen H.,Yang D.,2024:Review and Challenge: High Definition Map Technology for Intelligent Connected Vehicle. Fundamental Research.

Liu Y.,Song M.,Guo Y..2019:An incremental fusing method for high-definition map updating.IEEE , pp.4251-4256.

This contribution has been peer-reviewed.
https://doi.org/10.5194/isprs-archives-XLVIII-3-2024-301-2024 | © Author(s) 2024. CC BY 4.0 License.