

Research on the Security and Confidentiality System of Vehicle Owner Information in Urban Vehicle Dispatching System

Minghui Zhang^a, Yunhui Jia^b, Shunkai Wang^c and Wenbo Li^d

China Auto Information Technology Co., Ltd., Tianjin, 300000, China

^azhangminghui@catarc.ac.cn, ^bjiayunhui@catarc.ac.cn, ^cwangshunkai@catarc.ac.cn,

^dliwenbo@catarc.ac.cn

Abstract

At present, in various organs and enterprises of the society, many enterprises and units need to use vehicles. These vehicles can provide certain convenient services for the daily operation of enterprises and the travel of residents. However, in recent years, the information security leakage of the urban car dispatching system is very common, which also leads to the leakage of people's privacy, which even reduces the efficiency of vehicle use. At the same time, there are also a series of problems in the travel process of public vehicles. We improve the security of vehicle owner information in the urban vehicle dispatching system, and at the same time ensure that vehicles can be fully utilized. This paper also puts forward corresponding solutions for the research on the vehicle owner information security and confidentiality system in the urban vehicle dispatching system. After analyzing the current situation of vehicle scheduling and vehicle management in the city, the countermeasures to solve the vehicle owner information security and confidentiality are found.

Keywords

Car dispatching system; Car owner information security; Confidentiality.

1. INTRODUCTION

At present, the speed of urban development is accelerating, the standards of urbanization construction are improved, and the problem of traffic congestion in the city has become a key content that seriously restricts the development of the city [1]. City cars are the most important means of transportation to relieve traffic pressure. The management and dispatching efficiency of vehicles will affect the overall operation of cars and the convenience of people going out. Therefore, our reasonable scheduling and management of vehicles is of great importance to people's normal life, and the information security of vehicle owners in the urban vehicle scheduling system is particularly important. In actual deployment, we must ensure the security of these application operations. Even if there are dangerous nodes or attack nodes in the network, we must ensure that the security of the security application itself is not damaged, so as to ensure that the urban car dispatching system plays its positive role and prevent the dangerous operation of illegal nodes from bringing [2] greater harm to car owners. security risks, resulting in more serious losses.

The urban vehicle dispatching system has the characteristics of openness and high-speed mobility, which makes the vehicle nodes act as mobile, sensing and communication nodes in the network. In addition to common network attacks, we [3] will also face more security threats, such as the injection of false information in the urban car dispatching system, the tampering or replay of communication information, and the difficulty in detecting attacks by the system. In

addition, attackers may meet their own needs by publishing false information, and attackers can track other vehicles by eavesdropping on communication messages between vehicles. With the continuous advancement of the urban car dispatching system, the number of vehicles participating in the communication of the urban car dispatching system is increasing, and the scale and traffic flow of the urban car dispatching system will continue to expand. It is very important for the safety research under the environment of urban vehicle dispatching system. The importance of the application scenario of the urban vehicle dispatching system and the openness of the communication channel make it the main target of attackers from all walks of life. There are many problems when the traditional security strategy is directly applied to the wireless channel. If we use these The strategy is directly used in the special mobile self-organizing network [4] of the urban car dispatching system, and the urban car dispatching system will expose more loopholes and shortcomings. Therefore, researchers must combine the characteristics of the urban vehicle dispatching system to design a security strategy suitable for the characteristics of the urban [5] vehicle dispatching system. The designer needs to provide better security and defense measures under the condition of satisfying the basic functions of the urban vehicle dispatching system. See Figure 1.

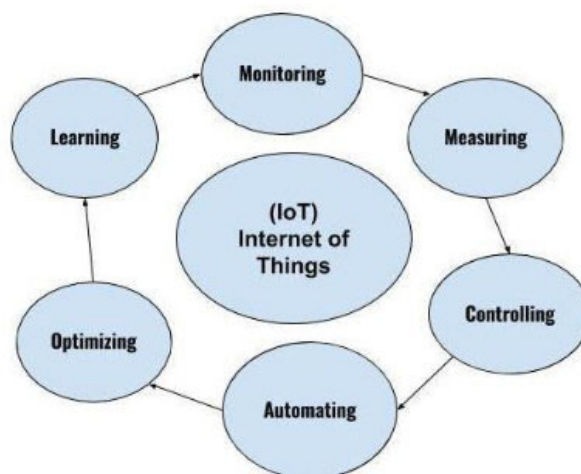


Figure 1. Intelligent car enterprise system under big data

2. THE FOCUS OF SAFETY RESEARCH UNDER THE ENVIRONMENT OF URBAN VEHICLE DISPATCHING SYSTEM

The urban vehicle dispatching system environment is mainly used in the public service system. Some applications may require the vehicle to send information related to its own identity for authentication, which provides an attack point for attackers. Therefore, the issues of user identity privacy, data privacy and location privacy in the urban vehicle dispatching system environment have gradually become the focus of researchers. In the urban vehicle dispatching system environment, vehicles obtain road traffic information by regularly exchanging information with roadside equipment and vehicles in the road network. The exchange frequency and aggregation degree of message packets are very high, and these message packets generally contain vehicle owners. The personal information and the movement status of the vehicle, which makes the car owners and vehicles in the urban car dispatching system face the hidden danger of privacy leakage. In addition, due to the rapid change of the network topology of the urban car dispatching system and the high centrality of vehicle nodes, these characteristics make it difficult to directly apply the traditional privacy protection scheme to the urban car dispatching system environment. Only by adapting the privacy protection strategy to the urban car dispatching system At the same time, we can hide the identity of the car owner, so that it can be effectively promoted among car owners, and the

city can further realize intelligent traffic control. The privacy protection technology in the urban car dispatching system environment was born under this background. Research on the security and confidentiality of vehicle owner information in urban vehicle Identity Privacy Protection in Urban Vehicle Dispatching System. Identity privacy protection has always been an important research direction of privacy protection in urban car dispatching systems. Generally, there are the following three methods:

2.1. Anonymous Authentication

Anonymous authentication is a relatively common privacy protection method. Some scholars have proposed an anonymous authentication scheme, which stipulates that the vehicle can show the authenticity of its identity to the authority through zero-knowledge proof. Some scholars have proposed an anonymous scheme based on shared certificates to realize identity verification between vehicles. This scheme reduces the number of vehicles using unique certificates in the same period to protect the privacy of users. These schemes implement anonymous authentication between vehicles without giving a method to reveal the anonymity of vehicles. In addition, some scholars have proposed a strong privacy protection two-factor authentication method based on node identity and trust. The method can ensure the security of the authentication process, the confidentiality of information and the privacy of vehicle nodes, and the method avoids the complex key management overhead through anonymity technology. However, this method improves the security of the authentication process by constructing complex interaction protocols between vehicle nodes. For the high-speed moving network nodes in the urban vehicle dispatching system environment, the real-time performance of this method needs to be further improved.

2.2. Pseudonym Technique

The pseudonym technology is an evolution of the anonymous technology. The main idea of the pseudonym technology is that the vehicle node uses the virtual identity issued by the trusted center to replace its real identity when communicating externally, which makes it impossible for other nodes to obtain its real identity. At the same time, in order to protect the privacy of the vehicle, when the vehicle uses a pseudonym, it must ensure that the attacker cannot contact the newly replaced pseudonym through the used pseudonym. This prevents the vehicle from establishing a link between the old and new pseudonyms. Therefore, the trusted center generally adopts a special pseudonym replacement strategy to make the vehicle change a new pseudonym at regular intervals, so as to ensure that the vehicle uses different pseudonyms in different time periods. In order to defend against the above possible attacks and solve the security risks of the urban car dispatching system, the urban car dispatching system must pay attention to the following information security requirements during the architecture and deployment process:

Authentication is the basic technology to defend against external attacks. Authentication is mainly divided into identity and message authentication. The recognition of identity realizes the screening of legitimate communication nodes, and the screening ensures that nodes in the network can judge whether their identities are legal when communicating with other nodes; the recognition of messages can help message recipients to judge the reliability and validity of message sources. See Figure 2.

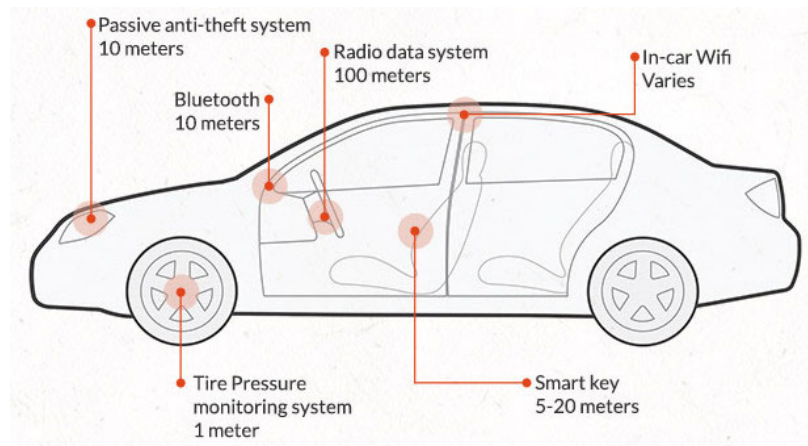


Figure 2. Automotive computer security system

Integrity means that the communication node must be able to judge whether the received message is complete or tampered, and the user can identify it from the source of the message and the forwarding process.

In the communication environment of the urban vehicle dispatching system, the identity privacy of the owner, the location privacy of the vehicle and the data privacy of the data packets sent must be protected.

The real identity of the node must be related to the identity of the node participating in the communication. This connection allows institutions such as the trusted center and the traffic control department to directly track their real identity, so as to ensure that people can be traced when relevant responsibilities need to be pursued. But we must ensure that the attacker cannot determine whether it is from the same car based on a series of behaviors in the network.

Non-repudiation.a communication node cannot deny that a message was sent or forwarded. When a communication node has a traffic accident or system loss due to operational errors or malicious attacks, it needs to be investigated for legal responsibility. This nature can assist relevant departments in tracing the cause of the accident.

3. REASONABLE SCHEDULING OF URBAN VEHICLES AND ANALYSIS OF VEHICLE MANAGEMENT

3.1. Outdated Scheduling Technology

The most important work content of urban automobile operation is the scheduling of automobiles. The rational use and scheduling of automobile resources in the city can ensure that this resource is used to the greatest extent. Putting into actual life and production work, cars bring convenience to people and improve the quality of work in the entire city. At present, many cities have a series of problems in the process of vehicle management and scheduling. These problems not only severely restrict the development of enterprises and undertakings to a large extent, but also affect people's daily life. These problems have caused obstacles to the operation of urban public transport.

3.2. The Transportation Efficiency Is Relatively Low

At present, most urban automobile passenger transportation hubs still use manual ticket sales, which will not only increase the workload of the staff, but also affect the ticket purchasing efficiency of car owners. At the same time, during the ticket checking process, we also completely rely on the staff to do it manually, which increases the time of car owners queuing, which also greatly reduces the efficiency of transporting car owners.

3.3. Station Safety Cannot Be Guaranteed

The safety of car owners is the most critical issue in urban automobile passenger transport hubs, but the monitoring systems, inspection systems, and security systems of some urban automobile passenger transport hubs are not perfect, and there is no effective connection between them, which leads to the emergence of some dangerous factors. , which poses a greater threat to the owner's information security.

4. COUNTERMEASURES OF THE OWNER'S INFORMATION SECURITY AND CONFIDENTIALITY SYSTEM IN THE URBAN CAR DISPATCHING SYSTEM

4.1. Improve the Network System to Achieve Full Coverage of Online Ticket Sales

Nowadays, the development of network information technology has greatly promoted the construction and improvement of the intelligent system of urban automobile passenger transport hubs, and the online and telephone bookings have greatly improved the ticketing efficiency of car owners. When the car owner's online or telephone booking is successful, the car owner only needs to enter or scan their ID card information at the car passenger hub to complete the ticket collection. It saves the travel time of passengers and also facilitates car owners to inquire about ticketing and vehicle information. We have realized the construction of the information system of the automobile passenger transportation hub. We can also promote the effective exchange of relevant information through the construction of the intelligent system of the automobile passenger transportation hub.

4.2. Improve the Intelligent Security Inspection System

For the urban automobile passenger transport hub, the intelligent security inspection system uses computer systems, fingerprint identification systems, RFID radio frequency identification systems and other related technologies to protect car owners from boarding to boarding. In fact, the intelligent security inspection system of the urban automobile passenger transportation hub can not only realize the protection of the life safety of the car owners, but also can manage the vehicles by storing the identification information of the vehicles. This will effectively reduce the probability of security risks. The intelligent security inspection system of the urban automobile passenger transportation hub can effectively supervise and manage vehicle owners, vehicles and related personnel to ensure the safe and efficient interactive transmission of relevant vehicle information. The intelligent security inspection system includes three functional modules: basic data management, vehicle management and dispatching center. See Fig. 3.

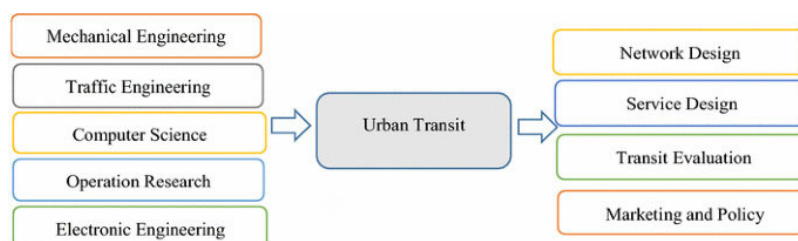


Figure 3. City Computer Vehicle Information Security and Confidentiality System

4.3. Increase the Innovation of Intelligent Technology

The automobile passenger transport hub has gradually abandoned the traditional operation mode, and the automobile passenger transport hub has begun to use cloud technology, big data and other new technical means to carry out the intelligent construction of the automobile passenger transport hub, so that the automobile passenger transport hub can better realize the timely and effective exchange of station information. The intelligent system of automobile

passenger transportation hub can realize the effective exchange of service information and passenger demand information with the help of network technology. Its functions include the following aspects:

4.4. The Intelligent System of the Automobile Passenger Transport Hub Can Conduct Online Ticketing and Remote Ticketing

The intelligent system can realize the online ticketing of passenger transportation in the city. The intelligent system promotes the construction of the business management system, data exchange management system, clearing and settlement system, and linkage ticketing service system. The intelligent system better realizes the exchange of information and Shared, intelligent system greatly facilitates car owners.

Weibo and WeChat are used to publicize and market the automobile passenger transport hub, and the owner can fully understand and master the relevant information of the vehicle by scanning the QR code. This not only facilitates car owners but also improves the operation efficiency of the automobile passenger transport hub.

WeChat Pay has built "Internet +" automobile passenger transport hubs in Beijing, Shanghai, Guangzhou, Guangdong, Haikou, Sanya and other regions. Car owners can get on the bus without collecting tickets, which greatly promotes the construction of intelligent systems.

The car owner generally generates three levels of information about the car owner's personal identity information, purchase relationship, and ticket purchase behavior during the ride. The urban car dispatching system organizes and analyzes these data to build a set of its own big data. The platform, the urban car dispatching system can better serve every car owner. In a word, with the development of the era of big data, if a car owner once took a car in the automobile passenger transportation hub, the relevant information of the car owner has been recorded, and the user can log in to the automobile passenger transportation hub network platform to view all the vehicle information of the user.

4.5. Network Collaboration to Achieve Information Security and Confidentiality

In the development of the information age, the automobile passenger transport hub needs an invisible platform as a support, so that the urban automobile passenger transport hub can have great cohesion, and the urban automobile passenger transport hub can win in the fierce market competition. Therefore, in order to promote the establishment of the automobile passenger transportation hub alliance, the urban automobile dispatching system needs to increase the network cooperation to realize the security and confidentiality of the information.

5. CONCLUSION

The rapid development of urban construction and the development of network information technology have effectively promoted the development of the transportation industry. The urban car dispatching system is an important part of the urbanization construction process. If the city wants to better meet the development needs of the times, it needs to promote the construction of the information security and confidentiality of the urban car dispatching system. Information confidentiality services during and after travel, which can not only promote the effective exchange of information but also improve the transportation efficiency of car owners. The car owner information security and confidentiality system in the urban car dispatching system protects the user's personal privacy from being leaked or violated.

REFERENCES

- [1] Li Aihua. Informatization construction of bus terminal is imperative. China Science and Technology Investment, Vol. 23(2017) No.23, p.83-84.2016, 7(20): 83-84.
- [2] Qian Chenglin. Exploration and practice of building an informationized comprehensive passenger transport hub. Science and Technology Prospects, Vol. 11(2018) No.13, p.121-122.
- [3] Tao Yafeng. Analysis on how to reasonably improve vehicle scheduling and vehicle management in government agencies. Small and Medium Enterprise Management and Technology, Vol. 3(2019) No.23, p.34-35.
- [4] Yu Yajun. A brief analysis of target control in vehicle dispatching in colleges and universities, Vol. 25(2018) No.23, p.51-52.
- [5] Xu Guoxin. Analysis of effective ways to strengthen fleet management and optimize vehicle scheduling. Science and Technology Innovation Herald, Vol. 25(2018) No.15, p.206-207.