Research on Security Communication Technology of Internet of Vehicles Based on 5G Technology

Shaojun Xiong
Wuhan Business University, Wuhan, Hubei Province, China

*Corresponding author e-mail: xsjleilei@hotmail.com

Abstract. With the improvement of the economic level and the development of infrastructure, the use of automobiles as a mode of transportation has become more and more common, and the number of cars has continued to grow. Based on this background, the rapid development of intelligent and networked automotive network communication technology, the birth of the Internet of Vehicles technology, has promoted the transformation of the automotive industry. This article gives the corresponding security requirements based on the security risks of IoV communication, briefly introduces the basic methods to realize the security of IoV communication, and proposes the service architecture, PKI architecture and multi-PKI system mutual trust mechanism to realize the security of IoV communication based on this.

Keywords: 5G technology, Internet of Vehicles, Secure communication, Communication technology.

1. Introduction
With the development of 5G communication technology, car networking industry has entered the fast lane, technological innovation is increasingly active, new applications are booming, and the scale of the industry continues to expand, but there are also key core technologies that need to be broken. Wireless communication technology plays a key role in the development of the Internet of Vehicles. In order to meet the reliability, transmission rate and capacity requirements of in-vehicle communication, vehicle communication needs to continuously improve and enhance the Internet of vehicles technology [1]. On the other hand, with the introduction of 5G technology, companies have devoted themselves to the research of high quality, high-reliability, and wide-coverage cellular Internet of Things technology. Based on the cellular Internet of Things technology, exploring the IoV communication of the end, tube, and cloud system is of great significance for promoting low power consumption, wide coverage, large connection and long battery life of vehicle communication, and also for promoting 5G applications and 5G joint innovation it has a positive meaning. This article analyzes the security threats and security requirements faced by IoV communications, briefly introduces the status of 3GPP V2X communication security standardization, proposes the service architecture and PKI architecture to realize IoV communications security, and looks forward to the development trend of IoV security technologies and standards [1].
Based on 5G-V2X and other technologies, a highly collaborative interconnected environment of “people, vehicles, roads, and clouds” will be built to realize advanced and autonomous driving such as vehicle-road collaborative control, vehicle-vehicle coordination, and remote operation. Behavior, and ultimately support the realization of fully automated driving. The research and development of Internet of Vehicles service applications has become very important.

2. Overview of the Safety Requirements of Car Networking Communication

Car networking short-range communication systems based on 4G-based LET-V2X technology or 5G-based NR V2X technology are faced with signaling risks such as counterfeit networks, signaling eavesdropping, signaling tampering, and signaling replay, but also face falsehoods security risks such as information, counterfeit terminals, information tampering, information replay, and privacy disclosure. In order to deal with the above-mentioned security risks, the Internet of Vehicles system should support the following main security capabilities [2]:

(1) Confidentiality requirements: The Internet of Vehicles system should be able to provide confidentiality protection for the transmitted data, to ensure that messages are not eavesdropped during transmission, and to prevent sensitive information from leaking [3].

(2) Integrity requirements: The Internet of Vehicles system should be able to provide integrity protection for the transmitted data to ensure that the message is not forged or tampered during transmission [3].

(3) Certification requirements: The car networking system should be able to support two-way authentication between terminals and between the terminal and the network, and the entities in the car networking system can verify the legality of data sources and data to prevent counterfeiting or forged data [3].

(4) Privacy protection requirements: The IoV communication system should provide a mechanism for hiding user identity information and location information to prevent the disclosure of privacy information such as user identity and location to unauthorized users [3].

3. Car Networking Safety Certification System

As a new generation of Internet and Internet of Things technology in the field of transportation systems, the Internet of Vehicles will undertake a large number of data communication tasks in future commercial applications. The communication security of the Internet of Vehicles can be divided into two categories according to its application areas: vehicle active safety system communication security and vehicle Internet application system communication security. In the vehicle active safety system, the vehicle broadcasts its driving status and location information at a given frequency to avoid collisions [4]. In this application scenario, it is necessary to provide authentication, integrity, non-repudiation, resistance to replay attacks, and privacy protection capabilities for the messages broadcast by the vehicle. In the Internet of Vehicles application system, it is necessary to provide authentication, integrity, and confidentiality protection capabilities for the messages broadcast by the vehicle according to the specific needs of the application [4].

3.1 Car Networking Communication Security Service Architecture

The Internet of Vehicles communication security service architecture is shown in Figure 1, which is composed of functions or entities such as full data processing functions, security credential management functions, security service functions, and security credential management [5]. Therefore, improving communication efficiency and increasing the communication volume per unit of time have become the focus of attention. However, with the development of Vehicles applications frequently involve sensitive information such as vehicle location and identity, the increase in communication volume has aggravated the leakage of user privacy data. The characteristics of IoV networking communication system determine a contradictory relationship between transmission efficiency and privacy security.
The security data processing function is located in an Internet of Vehicles application service entity in the Internet of Vehicles equipment, and is responsible for processing security operations related to specific applications, that is, generating and processing safety messages based on specific Internet of Vehicles application logic. For example, in the Internet of Vehicles active safety application, the vehicle active safety system generates a signature message or verifies a signature message based on the corresponding application logic [5]. SDPF may need to call basic security services provided by SSF in the process of secure data processing, such as digital signature, signature verification, data encryption, and data decryption. The security credential management function is located in the Internet of Vehicles equipment, and is responsible for interacting with the Internet of Vehicles security credential management entity to obtain related public key certificates and certificate revocation lists and other security credentials or data. SCMF needs to interact with SSF to complete the import and export of security data such as security credentials and CRL, as well as the generation and export of keys. The security service function is located in the Internet of Vehicles equipment, responsible for providing the storage of security credentials and security data and cryptographic calculation services, such as the storage of public key certificates and CRLs, the generation and storage of keys, signatures, verification, encryption, decryption and Harbin Greek calculations and other cryptographic calculations [5]. SSF provides external security services through the SSF application program interface. The security credential management entity is responsible for issuing various public key certificates for communication security and providing a certificate revocation list to the vehicle networking equipment.

3.2 The Security Process of Car Networking Communication
The general process of realizing the security of car networking communication is shown in Figure 2. Specific steps are as follows:
(1) The sender's SDPF generates plaintext data according to a certain car networking application logic, and sends a security service request to the local SSF so that the latter can provide security services such as digital signature or data encryption. The service request contains plaintext data and/or data required to process the security protocol data unit, such as a public key certificate [6]. (2) The SSF of the sender performs corresponding security operations, such as data signing or data encryption, according to the security service request. The SSF encapsulates the result of the safety operation in the SDPU, and then returns the SDPU to the SDPF through the safety service response. (3) The SDPF of the sender generates a safety message in an application-specific format according to the SDPU generated by the SSF and application logic, such as an active safety message [6]. (4) The SDPF of the sender broadcasts the generated safety message. (5) The receiver's SDPF obtains the SDPU from the received safety message according to the application logic. (6) The receiver's SDPF sends a security service request to the local SSF so that the latter can provide security services such as signature verification or data decryption [7]. The service request contains the SDPU and/or data required to process the security protocol data unit, such as public key certificates. (7) The SSF of the receiver performs corresponding security operations according to the security service request, such as verifying signatures or decrypting data, etc., and then returns the security service result to SDPF through the security service response.

3.3 Certificate Type
According to the purpose of the car networking communication certificate, the certificate can be divided into four types: CA certificate, registration certificate, pseudonym certificate and application certificate. A CA certificate (CA Certificate) is a certificate issued by a certificate authority (CA) that issues registration certificates, pseudonymous certificates, or application certificates. The root CA certificate (Root Certificate) is a self-signed certificate, which is the root node of all certificate chains of a PKI system, and is called the trust anchor of a PKI system [7]. The root CA can issue sub-CA certificates to subordinate CAs as needed, such as registered CA certificates, pseudonymous CA certificates, and application CA certificates. The registered CA issues enrollment Certificate (Enrollment Certificate) to the connected car equipment. After the connected car equipment is certified by the registration agency, the registration CA will issue a registration certificate for it. The registration certificate uniquely corresponds to the device. The device needs to use the registration certificate to apply for a communication certificate suitable for a certain application field from other authorization agencies (Authorization Authority, AA). The pseudonym certificate (Pseudonym Certificate) is issued to the OBU by the pseudonym CA. OBU uses a pseudonymous certificate to sign the active safety message (Basic Safety Message, BSM) it broadcasts. In order to protect user privacy, it is necessary to use password technology to encrypt the user's identity information [8]. OBU can have multiple pseudonymous certificates, which can be used to switch regularly, so as to avoid revealing the driving track of the vehicle. The Application Certificate (Application Certificate) is
issued by the application CA to the RSU or the Internet of Vehicles application service provider (Service Provider, SP), which is used in a specific Internet of Vehicles application field. RSU uses application certificates to sign certain application messages it broadcasts. For example, RSU uses application certificates to issue traffic signal status, traffic information, commercial service messages, etc. that it broadcasts [8]. For a specific car networking application, RSU can only have one application certificate. Identity Certificate (Identity Certificate) is issued by the application CA to the OBU, which is used in a specific Internet of Vehicles application field.

Limited by wireless statistical technology, the existing 3G/4G communication-based vehicle networking authentication mechanism is applicable to a single communication scenario, which mainly includes identity authentication for the legitimacy of vehicle node identity, and static and dynamic attributes for a specific identity. Authentication and authentication for messages transmitted between entities lack a comprehensive consideration of multi-communication scenarios. After investigation, this paper find that most of the current research on privacy protection is mainly carried out at the communication protocol level, and the ability of privacy protection is improved by improving the existing security mechanisms. Below we introduce the identity authentication technology based on the trusted platform module.

3.4 PKI Reference Architecture
A PKI architecture for issuing various communication certificates to connected car devices is shown in Figure 3. The PKI architecture includes five types of authorized entities: root CA, registered CA, pseudonymous CA, application CA, and certificate revocation authority.

![PKI architecture](image)

**Fig.3 PKI architecture for issuing various communication certificates**

Root CA (Root CA) is the highest level CA in a certain PKI system in the Internet of Vehicles security system. The root CA can issue sub-CA certificates to subordinate CAs as needed, such as registered CA certificates, pseudonymous CA certificates, and application CA certificates. Enrollment CA (Enrollment CA, ECA) is responsible for issuing registration certificates to car networking equipment such as OBU and RSU. In order to join a certain IoV application, IoV devices such as OBU and RSU first need to pass the certification of the registration agency and obtain the registration certificate, and then use the registration certificate to apply to the application authority (application CA) for the communication that is actually used to generate the IoV safety message certificate [9]. In a car networking PKI system, different registered CAs can be set up according to different application fields and management scopes to manage the access of devices in related application fields. OBU uses a pseudonymous certificate to digitally sign the active safety message (Basic Safety Message, BSM) it broadcasts [9]. To avoid disclosing the driving path of the vehicle, PCA should issue multiple pseudonymous certificates to OBU; OBU regularly replaces the certificates used for message signing.
According to the pseudonymous certificate usage policy. Application CA (Application CA, ACA) is responsible for issuing application certificates suitable for a certain car networking application field to RSU or SP and issuing identity certificates suitable for a certain car networking application field to OBU. Certificate Revocation Authority (Certificate Revocation Authority, CRA) is responsible for managing and issuing Certificate Revocation List (CRL) of issued certificates [9].

3.5 Support for Mutual Trust among Multiple PKI Systems

When the Internet of Vehicles security system is composed of multiple independent PKI systems, these PKI systems can build a mutual trust relationship as needed to achieve mutual recognition of certificates [10]. The mutual trust relationship between multiple car networking PKI systems can be realized through a trusted certificate list (Certificate Trust List, CTL).

The existence of CTL will not affect the operation of each independent PKI system, but it will affect whether the certificates of different PKI systems can be mutually recognized. The Internet of Vehicles system can dynamically add or remove the root CA certificate from the CTL as needed. When the new CTL is generated, the old CTL is automatically invalidated [10].

4. Conclusion

Overall, 5G is getting closer and closer to us. As an application scenario of 5G, the Internet of Vehicles has gradually matured with the rapid development of 5G technology. Driven by 5G technology, through network evolution and upgrades to support low-latency and high-reliability communication services in the Internet of Vehicles, future transportation will inevitably develop in the direction of more intelligent and grid-based. At the same time, operators are also actively exploring the role change in the newly formed smart transportation industry chain that is, evolving from traditional pipeline services to full-service operations. It is believed that the development of 5G Internet of Vehicles can promote the great evolution of society, and make human society more convenient, safer, faster and more efficient. The research direction of this project is the privacy and security protection of the Internet of Vehicles communication system, and fully considers the problems and challenges faced by the Internet of Vehicles in 5G communication application scenarios, and plans to study the communication security protection mechanism of the Internet of Vehicles; and will adopt the idea of game theory. To conduct in-depth research on the effective combination and balance of communication efficiency and security.

Acknowledgement

Foundation Project: University-level scientific research project of Wuhan Business University, Project Name: Research on Communication Security Mechanism Based on 5G Internet of Vehicles (Project No. 2019KY030).

References

[1] Xiang, H.Y., Zhang, X.R. and Pu, Zh.Y: 5G mobile communication system access network architecture. Telecommunications Science, 11(08), 15-18(2018).
[2] Dong, A.X. and Wang, X.J.: 5G Communication Technology and Development Trend. Communication Technology, 7(03), 235-238(2017).
[3] Li, Y.: IoV technology and intelligent connected cars based on 5G mobile communication. China Information Technology, 8(06), 124-127(2019).
[4] Meng, M.: Application Research of 5G Communication Technology in Heterogeneous Vehicle Networks. Digital Communication World, 12(04), 169-172(2019).
[5] Wei, Y.: Research on the development of Internet of Vehicles based on 5G communication technology. Southern Agricultural Machinery, 10(13), 223-225(2019).
[6] Huang, H.X.: Research on the Security of the Internet of Vehicles System Based on MEC. Information Security and Communication Confidentiality, 13(06), 88-91(2020).
[7] Li, W.J.: Design of a car network monitoring system based on laser scanning. Laser Magazine,
13(05), 178-182(2020).

[8] Zheng, X., Liu, Y. and Ke, J.Q.: Research on Cluster Head Selection and Data Transmission Strategy Based on Fuzzy Logic in Internet of Vehicles. Information Security and Communication Secrecy, 41(07), 1458-1460(2020).

[9] Xie, Sh.: Combination and development of LTE wireless communication technology and Internet of Things technology. Science and Wealth, 12(05), 87-90(2018).

[10] Cheng, L.L., Ding, K. and Wu, X.D.: Intelligent vehicle networking simulation platform promotes the healthy development of smart transportation. China Automatic Identification Technology, 2019 (5): 63-66.