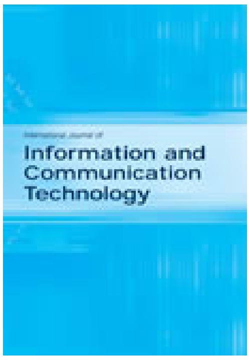


International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Research on over-the-air programming and real-name authentication technology of eSIM based on 5G communication technology

Jun Lu, Guowei Huang, Liangjie Cui, Pengcheng Zhang

Article History:

Received:	17 June 2024
Last revised:	25 September 2024
Accepted:	26 September 2024
Published online:	31 March 2025

Research on over-the-air programming and real-name authentication technology of eSIM based on 5G communication technology

Jun Lu, Guowei Huang*, Liangjie Cui and Pengcheng Zhang

Information and Communication Branch of
State Grid Anhui Electric Power Co., Ltd.,
Hefei, China
Email: luj2014@ah.sgcc.com.cn
Email: hgw201436@outlook.com
Email: ncepuclj@163.com
Email: 842909653@qq.com
*Corresponding author

Abstract: The emergence of eSIM card is another evolution of SIM card, and it is also in line with the technical development direction and market demand of SIM card from large to small and from real to virtual. This paper aims to combine 5G communication technology to study the over-the-air programming and real-name authentication technology of eSIM, and proposes a new random access design for the long delay and rapid timing advance (TA) change characteristics of low-orbit satellite communication system. Moreover, this paper proposes a random access preamble structure based on polarity expansion and a new TA adjustment strategy based on downlink tracking. In addition, this paper designs a random access response data structure suitable for LEO satellite environment at the protocol layer, and builds a blockchain eSIM solution architecture design system based on 5G communication. Finally, this paper verifies the effectiveness of the technology proposed in this paper combined with experimental tests, thus providing a theoretical reference for subsequent related research on the popularisation of eSIM to user groups.

Keywords: 5G; communication technology; eSIM; over-the-air programming; real-name authentication.

Reference to this paper should be made as follows: Lu, J., Huang, G., Cui, L. and Zhang, P. (2025) 'Research on over-the-air programming and real-name authentication technology of eSIM based on 5G communication technology', *Int. J. Information and Communication Technology*, Vol. 26, No. 6, pp.21–44.

Biographical notes: Jun Lu is a Master degree candidate in University of Science and Technology of China and Senior Engineer. His main research interests are 5G communication, wireless communication, power communication. He participated in the research and development of a smart collaborative management model based on self-organising networks, undertaking project control and related research work. This project achieved intelligent management of equipment, construction of system routing networks, automatic frequency planning, interference coordination between sites, and full network topology management, enhancing the efficiency of equipment usage and improving the level of communication support.

Guowei Huang is a Master degree candidate in Central South University and Junior Engineer. His main research interests are power communication, data communication network and signal processing. He has participated in the research and application of performance improvement technologies for self-organising networks in terms of transmission and reception efficiency, and he has taken on the implementation of the projects. His main research focuses on how to solve problems such as signal distortion and inter-symbol interference during the processing at the receiving or transmitting end, thereby enhancing the performance and reliability of communication systems.

Liangjie Cui is a Master degree candidate in North China Electric Power University and Junior Engineer. His main research interest is power communication. He has participated in the research and application of performance improvement technologies such as self-organising network transmission and reception efficiency in projects, undertaking project implementation and related research work. Based on a comprehensive review of typical power business requirements, he has conducted feature extraction and classification of power business, extracted network requirements, and studied lightweight communication network evaluation methods for intelligent perception of power business quality. This provides a secure and reliable access means for power business.

Pengcheng Zhang obtained his Bachelor's degree from the School of Electronic and Information Engineering at Tianjin University of Technology in 2016, and Master's in Communication Engineering from Nankai University in 2018. He is currently working at the State Grid Anhui Information & Telecommunication Company. His research mainly focuses on power communication, and he has been dedicated to research in the field of power communication, accumulating rich practical experience and profound technical expertise. He participated in the research and development project of the intelligent collaborative management mode based on self-organising networks, taking on the role of project leader.

1 Introduction

In the process of internet of things (IoT) business development, major operators have developed related dedicated embedded IoT cards, which are not only the carrier of operators' code resources, but also the identity certificate for IoT product terminals to access wireless communication networks. According to the statistics released by ABI Research, the number of various dedicated IoT SIM cards used in the internet of things in 2008 was about 60 million, and this number had increased to 200 million by 2014. Therefore, with the rapid development of the IoT business, the development and demand of embedded IoT cards are faster and higher, and their applications in internet of vehicles, food traceability, environmental monitoring, smart home and other aspects are becoming more and more extensive.

Compared to regular cards, the cards used by Wuzhen.com generally use higher standards. The lifespan of ordinary cards used in mobile phones is generally 3–5 years, after which they are prone to malfunctions (Apilo et al., 2022). However, some IoT application scenarios (such as intelligent meter reading in the hydropower and coal industry) require embedded cards to have a normal working state of at least ten years.

Ordinary IoT cards cannot fully meet the industrial level requirements of special IoT application environments for cards, such as anti-theft requirements, to prevent SIM cards in IoT terminals from being pulled out and diverted to other illegal businesses; seismic requirements, especially in the application scenarios of connected vehicles, are particularly sensitive to moisture. Cards often vibrate during operation, making them prone to poor contact or damage; in terms of card erasure frequency, in ordinary business application scenarios, card erasure occurs mainly when the machine is turned on or the device position is changed. However, in the field of IoT applications, high-density data collection scenarios are everywhere, and terminal erasures of cards are more frequent, resulting in a higher frequency of use (Vikhrova et al., 2022). Due to the exponential growth of IoT applications in the aforementioned scenarios, the number of IoT embedded cards is also increasing exponentially. These factors have led to a sharp increase in the demand for IoT embedded cards to be opened in the air. The activation or deactivation of embedded IoT cards is quite different from that of regular SIM cards. Generally, in order to improve the reliability and stability of communication, embedded IoT cards are soldered onto the internal circuit board of IoT product terminals during the production process. Therefore, theoretically, embedded IoT cards should not be removed or replaced after being embedded in IoT terminals, as such maintenance costs can be quite high (Kim et al., 2020). Therefore, how to read and open embedded IoT cards anytime and anywhere while meeting different business requirements has become an urgent issue. For example, the electricity meter factory has produced a batch of smart meters equipped with embedded IoT cards. In many cases, the smart water meters do not immediately open for service after entering the household. Generally, it is necessary to wait for the residents to move in before officially opening the service. At this time, like traditional communication services, unplugging the SIM card and going to the operator's business hall to read and write information to open the service becomes very troublesome and unrealistic. At this point, opening and changing the business can be completed very well by opening the card in the air (He et al., 2021).

Aiming at the problems existing in the current eSIM over-the-air programming and real-name authentication technology, this paper aims to improve it in combination with 5G communication technology, and innovatively build a blockchain eSIM solution architecture design system based on 5G communication. At the same time, this paper verifies the effectiveness of the technology proposed in this paper combined with experimental tests. The contribution of this paper is to provide a theoretical reference for the popularisation of eSIM to user groups for subsequent related research.

2 Related work

Over-the-air technology, also known as OTA, is a technology for opening cards in the air. It is a technology that remotely manages data or applications in SIM cards issued by operators through the air interface of mobile communication networks (GSM, WCDMA, CDMA networks) (Borgaonkar et al., 2021). The air interface can use short message technology, GPRS, WAP, and CAMA1X technology. The application of aerial card opening technology not only limits mobile communication to traditional voice and data services, but also provides new services such as card data management and new business downloads. Japan was the first to propose air download technology. At that time, the explosive growth in the number of mobile communication users posed increasingly high demands on both mobile phones and communication technology. Mobile phones are constantly developing towards greater intelligence and multimedia, while newly launched phones are equipped with stronger processing capabilities and pre installed with the most commonly used applications such as browsers and media players. Some phones even had cameras at that time. These emerging mobile phones have more powerful and diverse functions, but they are often more prone to malfunctions compared to older phones with a single call function. Sometimes, it may lose internal data or crash like a computer, while also being threatened by mobile phone viruses. When similar situations occur, mobile phone manufacturers must recall faulty phones in accordance with relevant Japanese regulations, which will increase the additional cost of mobile phone production and sales (Medeiros et al., 2024). In order to easily update the system software in the problematic mobile phone without recalling the mobile phone, the groundbreaking concept of over the air download technology came into being. Its biggest function is to remotely manage the data or built-in applications of the mobile phone or card through the air interface of the mobile communication network (GSM, CDMA), so that the mobile phone can easily update the mobile phone system by wireless download, just like the computer downloads software through the internet (Khalid et al., 2022). To reduce the occupancy rate of number resources, remote card writing can be used to write number data when users open accounts. Unlike card making and number writing in a card factory, remote card writing is an operation in which an operator sends data to the point of sale (POS) through a remote server when a user opens an account, and then writes the number data to the SIM card in real-time. Card factory card making and number writing involves mass production of a batch of cards with already written number data, and then returning these finished cards to the operator for operation one by one (Luglio et al., 2022).

When writing numbers remotely through POS, the essence is to distribute the batch number writing operations of the factory in the business hall or some agency points, and the number resources are allocated in real-time when activated by users, effectively improving the utilisation rate of number resources (Lin et al., 2021). The usual remote card writing method requires the use of POS, which can be divided into two types:

1 Wired method: POS connects to the network through a computer, enabling connection with a remote card issuing server; the local computer calls the number writing module based on the number data pushed by the remote card issuing server, and drives the POS to perform number writing operations on the SIM card. The entire process is carried out in the form of a wired network, usually requiring computer configuration (Casetti, 2022).

2 Wireless mode: this method is carried out through a customised POS that can log in to the mobile network. This POS usually has two card slots. One SIM card slot device is used to connect to the network through POS login and obtain remote card issuing server write data, while the other slot is used to write new cards (Suomalainen et al., 2021).

Due to not relying on computers, the POS is also equipped with a keyboard, display screen, and even a printing device. The wired method is usually deployed in business halls and is inevitably limited by geographical location, which affects the customer development of operators. This method is basically not feasible (Demirev, 2020).

Compared to wired methods, wireless methods are much more flexible, and agents only need a wireless card writing POS to complete customer development (Mishra et al., 2021). This method does not require computer support, and the connection is made wirelessly over the air. In fact, some operators have already implemented this wireless POS card writing method and achieved good results (Dymkova, 2021). Although the aerial card writing method of wireless POS is relatively convenient, it is suitable for operators to develop customers in areas that cannot be covered by the business hall. The operation and maintenance cost of the system is also similar to a universal mobile phone-based aerial card writing method. Currently, research focuses on access control and network selection in wireless heterogeneous networks (Praveen et al., 2020). Ibarrola et al. (2023) propose a Bayesian decision-based vertical switching algorithm that takes into account signal strength, network load, bit error rate, and user information flow needs and preferences to ensure high-quality services. Abdel Hakeem et al. (2020) adopt a load and service adaptive algorithm in an integrated UMTS/WLAN network environment, which achieves breakthroughs in connection blocking rate and system resource utilisation. Mao et al. (2021) propose a network selection scheme based on latent games, and uses learning automata to assist in learning Nash equilibrium through limited feedback. In order to improve the quality of network selection and reduce switching times, Tusha et al. (2020) propose an improved CRITIC algorithm based on the comprehensive weight of user subjective preferences and network performance. Fan et al. (2021) proposes a vertical switching network selection mechanism, including weight allocation and pricing factors, which can seamlessly access the network at all times and meet the needs of users. By modelling heterogeneous networks as Markov decision processes and using heuristic matching algorithms, a user centred wireless access and service matching mechanism is introduced in Su (2021).

The development of SIM cards has progressed from standard SIM (initial card) to micro SIM (mini card) and now to nano SIM (ultra small card), with the size of SIM cards becoming increasingly smaller. The emergence of eSIM tells the market that the physical form of SIM cards will gradually be phased out, and the development of eSIM will be the trend. According to survey data, the shipment volume of eSIM supported communication devices is expected to reach between 3 billion and 8 billion by 2020. In 10 years, the shipment volume of communication devices using detachable SIM cards on the market will decrease by more than 15%, which means that the technological development of eSIM will be unstoppable in the future.

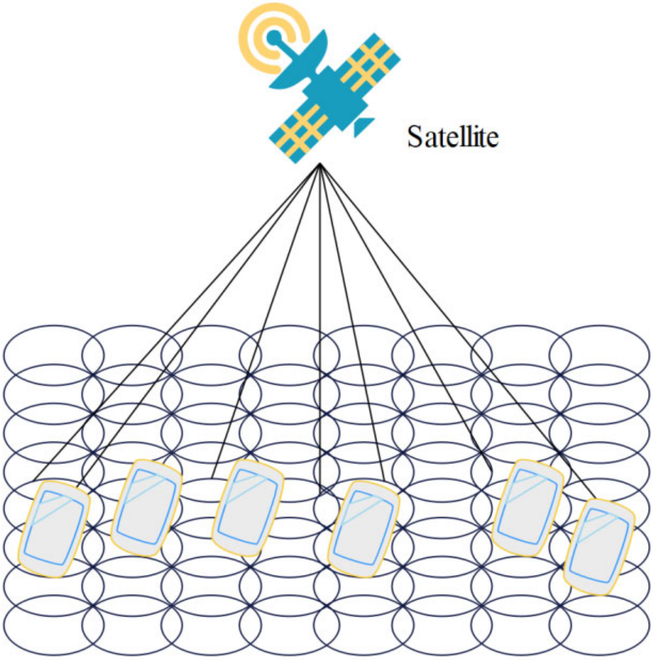
3 Access design scheme of over-the-air programming of eSIM

LEO satellite mobile communication uses a protocol stack based on ground communication. The existing ground communication protocol stack is relatively mature and runs stably, but it is designed based on the application scenarios of ground objects, and is suitable for objects whose movement speed is smaller than the speed of bullet trains, and the coverage distance of a base station does not exceed 100 km. However, the motion speed of the low-orbit satellite mobile communication system far exceeds that of ground objects, and the distance covered by satellites is far more than 100 km.

3.1 System scenario model

In this paper, the round-trip transmission delay difference in each group of beams is set as 3 ms, so the beams can be divided into three groups, and the transmission distance difference of each group is 450 km. Considering the overlap between different packets, the first group is the transmission distance of 727–1,180 km beams, the second group is the transmission distance of 1,150–1,600 km beams, and the third group is the transmission distance of 1,600–1,800 km beams, as shown in Figure 1. In Figure 1, signal transmission is carried out through airborne satellites within their coverage areas. There are multiple coverage areas in the figure, and user terminal devices within these areas can receive the corresponding signals.

Figure 1 Schematic diagram of multi-beam coverage of LEO satellites (see online version for colours)



For the satellite mobile communication system, the satellite and mobile terminal have a large propagation distance and pass through the atmosphere, which will be subject to a variety of attenuation, mainly including free space path loss, atmospheric scintillation, rain attenuation and gas absorption. Especially for the Ka-band satellite transmission channel, the transmission reliability of the communication system is poor and the transmission performance is unstable under severe weather, which is greatly affected by rainfall and other weather. In the process of satellite mobile communication, due to the relative motion of the satellite and the mobile terminal, the frequency of the signal arriving at the receiving end is offset, which is called the Doppler effect. The formula for calculating the Doppler frequency offset is:

$$f_d = \frac{v}{\lambda}\cos\alpha = f_c\frac{v}{c}\cos\alpha = f_m\cos\alpha \tag{1}$$

Among them, f_c is the carrier frequency, c is the speed of light, v is the moving speed of the ground terminal relative to the satellite, α is the angle between the direction of arrival and the direction of motion, and f_m is the maximum Doppler offset. According to the scene model described in Figure 2, the satellite is located in a low altitude area and follows a predetermined orbit. Below the satellite are ground observation points and the horizon. The relevant angles between the satellite and the horizon, as well as the vertical line from the satellite to the centre of the earth, are marked in the figure. The Doppler frequency offset change during the overhead process of a low-orbit satellite is calculated. Figure 3 shows that the ground terminal is located on the sub-satellite point trajectory of this satellite orbit. The figure marks the mutual position and angle between targets such as satellites, receivers, and the Earth.

It can be obtained that the distance between the satellite and the ground receiver can be expressed as:

$$d = \sqrt{rE^2 + \left(h + r_E\right)^2 - 2\cdot r_E \cdot \left(h + r_E\right)\cdot\cos\alpha} \tag{2}$$

In this expression, the distance between the satellite and the terrestrial receiver is expressed as a function of the geocentric angle α. Therefore, we can obtain:

$$V_T = -\frac{1}{2}\frac{2r_E\cdot\left(h + r_E\right)\cdot\sin\alpha}{\sqrt{rE^2 + \left(h + r_E\right)^2 - 2\cdot r_E\cdot\left(h + r_E\right)\cdot\cos\alpha}}\cdot\frac{d\alpha}{dt} \tag{3}$$

Figure 2 Schematic diagram of downlink coverage of LEO satellites

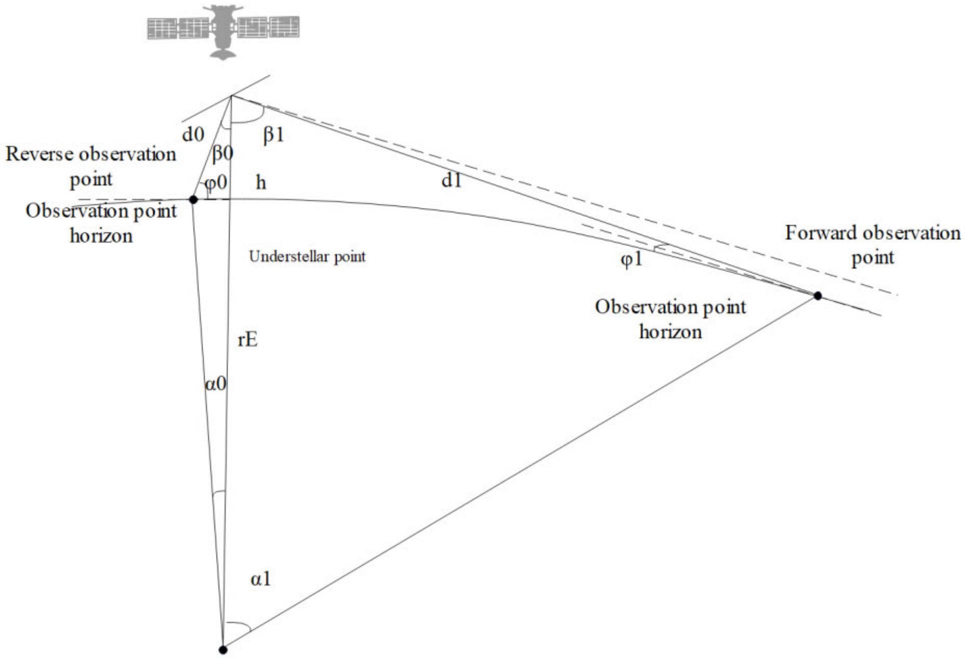
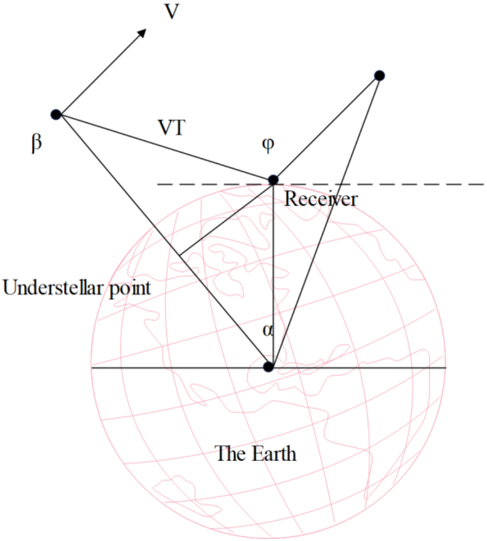

d0
β1
Reverse observation point
β0
φ0
h
d1
Observation point horizon
Understellar point
Forward observation point
φ1
Observation point horizon
rE
α0
α1

Figure 3 Schematic diagram of Doppler frequency offset calculation (see online version for colours)



Among them, $\frac{d\alpha}{dt}$ is the angular rate of the satellite, that is, the angle travelled in unit time, which can be expressed as:

$$\frac{d\alpha}{dt} = \sqrt{\frac{\mu}{(h + r_E)^3}} \tag{4}$$

Among them, μ is Kepler's constant. If the carrier frequency is assumed to be 30 GHz, the formula for calculating the Doppler frequency offset can be written as $f_d = f_c \frac{V_T}{c}$, where f_c is the carrier frequency, v is the flight speed of the satellite, and c is the speed of light. Further, the Doppler rate of change may be expressed as:

$$\begin{aligned} \frac{df_d}{dt} &= \frac{f_c}{c} \cdot \frac{dV_T}{dt} \\ &= \frac{f_c}{c}\left(\frac{r_E \cdot r \cdot \cos\alpha}{\sqrt{rE^2 + r^2 - 2 \cdot r_E \cdot r \cdot \cos\alpha}} - \frac{(r_E \cdot r \cdot \sin\alpha)2}{(rE^2 + r^2 - 2 \cdot r_E \cdot r \cdot \cos\alpha)^{3/2}} \right)\frac{\mu}{r^3} \end{aligned} \tag{5}$$

Among them, $r = h + r_E$. In addition, the relationship between the geocentric angle and the elevation angle of the ground observation point can be obtained from Figure 2 as follows:

$$\alpha = \arccos\left(\frac{r_E}{h + r_E} \cdot \cos\varphi \right) - \varphi \tag{6}$$

The change process of Doppler frequency offset and Doppler rate of change during a low-orbit satellite overtopping is shown in Figure 4. From the graph, it can be seen that Doppler shift shows an upward trend with elevation, while rate of Doppler shift shows a normal distribution trend with elevation.

3.2 Design of preamble sequence and random access response

The transmission delay of the LEO satellite system is much larger than that of the ground system. If the frame structure and sequence design of the ground mobile communication system are directly used, the satellite mobile communication system will not be able to obtain the correct timing, so the whole system cannot work normally. Therefore, it is necessary to redesign the random access sequence and structure of the satellite communication system. Random access sequence structure diagram for four different configurations is shown in Figure 5. This figure provides several corresponding forms of the corresponding model.

In order to be compatible with the ground mobile communication system, the random access sequence uses the PRACH preamble sequence of the LTE system as the extended base sequence (which can be expanded according to the preamble sequence defined by the 5G NR specification), and the frequency domain sequence is generated by the ZC sequence. Its length is $N_{ZC} = 839$, the time domain sequence length is $N_{IDFT} = 24,587$, and the corresponding sequence time is 0.8 ms. In order to simplify the discussion, only the beam on the trajectory of the point below the satellite is considered. We assume that the orbit altitude of the satellite is 727 km, the maximum transmission distance at the edge is 1,800 km, that is, the distance between the satellite and the ground user varies from 727 to 1,800 km, and the transmission delay of the satellite at the farthest point is 6 ms, and the transmission delay at the top is 2.4 ms.

Figure 4 Doppler frequency offset and Doppler rate of change curves (see online version for colours)

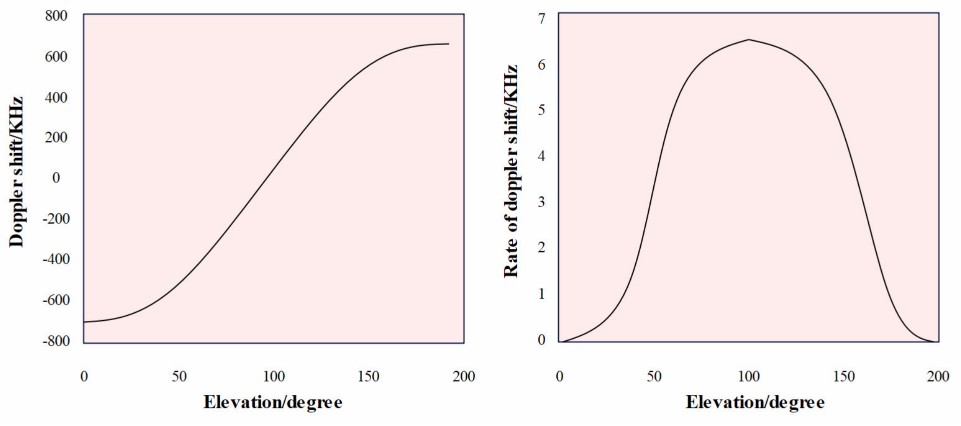
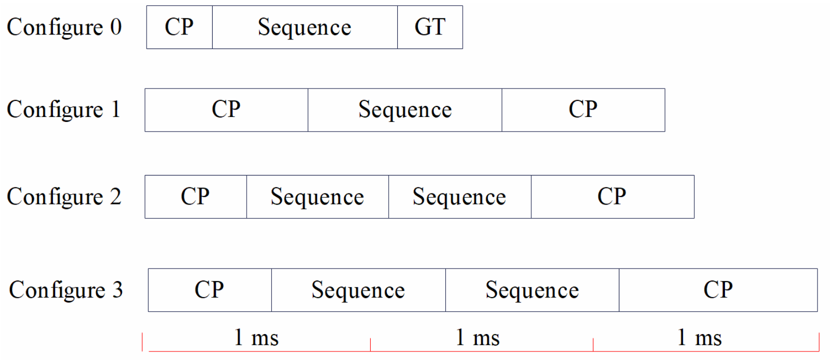


Figure 5 Random access sequence structure diagram for four different configurations (see online version for colours)



Firstly, the beams are grouped according to the transmission distance, so that the maximum transmission distance within each group is controlled within a certain range. The round-trip transmission delay difference within each group is set to 3 ms, and the starting position of the random access detection window for each group is set at the receiving end based on the minimum round-trip transmission delay value. In addition, due to the maximum round-trip transmission delay of 12 ms in this system, the system can initiate random access every two frames, that is, every 20 ms.

Redesign the random access sequence. In satellite mobile communication systems, the structure of the random access sequence is consistent with that of the ground communication system, consisting of CP, sequence, and GT. The design of these three parts must meet the following points:

1 To maximise the number of orthogonal leading sequences, a single sequence must be as long as possible, but considering system overhead and random access frame duration limitations.

2 To ensure ranging accuracy and effective discrimination, the sequence length must be greater than the CP length.

3 The subcarrier interval of the uplink must be an integer multiple of the PRACH subcarrier interval.

4 Considering coverage performance, the duration of the sequence can be calculated by the ratio of the required energy of the leading sequence to thermal noise, and satisfies the target missed detection probability and false alarm probability.

5 The length of the CP needs to be greater than the sum of the maximum round-trip propagation delay and the maximum delay extension. The complete sequence of user 3 cannot be observed within the detection window, which leads to incorrect detection and access failure.

6 In order to avoid aliasing between randomly accessed data and the next frame data, the length of GT must prevent symbol interference caused by dragging the current frame data to the next frame.

7 In order to be compatible with the ground mobile communication system, the preamble sequence is extended from the PRACH preamble sequence of the ground mobile communication system. In summary, the length of the preamble sequence is set to 3.2 ms, which is obtained by repeating the 800 us short sequence of the ground PRACH four times through symbol extension; the CP length is set to 3 ms, which is the loop leading end data of the leading sequence, and the GT length is set to 12 ms.

In the sequence design process, if the original preamble sequence is repeated four times directly as a new sequence, on the receiving side, the sequence of user 1 and user 2 is completely consistent in the observation interval, resulting in ambiguous ranging and inability to effectively distinguish the two. Therefore, a new sequence is obtained by Kronecker multiplication between a simple extended sequence and the original leader sequence. The designed extended sequence is as simple as possible, and the values of elements are composed of {+1, –1}. At this time, the expansion of the leading sequence can be expressed as equation (7).

$$\widehat{S} = W \otimes S \tag{7}$$

3.3 TA downlink tracking and timer configuration

Timing advance (TA) is a command sent by the base station (BS) to the UE to adjust its uplink transmission, that is, the user equipment (UE) sends uplink symbols in advance according to the commands used for physical uplink shared channel (PUSCH), physical uplink control channel (PUCCH), and sounding reference signal (SRS) transmission. The TAC (timing advance command) notifies the UE of the amount of time it needs to advance the uplink transmission.

Physical random access channel (PRACH) is the access channel used by the UE when initiating a call. After receiving the FPACH response message, the UE will send an RRCConnection request message on the PRACH channel based on the information indicated by the NodeB to establish an RRC connection.

The rapid movement of LEO satellites leads to continuous changes in TA and the current TA is estimated to have undergone major changes in the next data reception process, so TA cannot be adjusted in real time. For example, the base station receives the uplink PRACH data for detection, and sends the TA to the user. The user receives the TA for adjustment and transmits the uplink data. Then, the base station receives the uplink data for detection. The delay between this process has caused the uplink timing of the base station to change.

As shown in Figure 6, the random access process T_n to T_{n+1} indicates that at a time of 10 ms in a system frame, the first step UE sends a random access preamble sequence to the satellite and arrives at the satellite at time 1 in Figure 6. Due to the use of a newly designed longer preamble sequence, the satellite’s PRAcH reception and detection time is relatively long. We assume that it is 15 ms, the satellite sends a random access response to the UE at time 2, and arrives at the UE at time 3 after 6 ms, which contains TA commands. After receiving the TA command, the UE makes TA adjustments, and the time required for this process is the same as that of the ground system as the UE. After adjusting the TA, the UE sends its identity on the time-frequency resource indicated by the random access response at the third step of random access at time 4, and the message reaches the satellite after 6 ms. It can be seen that at the time T_3, the satellite receives the information from the UE for the first time, and when the satellite receives the data from the UE for the second time, it is already a code time, and the period is 30 ms different. In the process, the position of the satellite has changed a lot. Moreover, the TA adjusted by UE is based on the distance between the UE and the satellite at the time T_0. Using the uplink in advance for the dead time will cause relatively large errors, and the calculation of the errors will be discussed in the following content.

Figure 6 Random access process under LEO satellite conditions

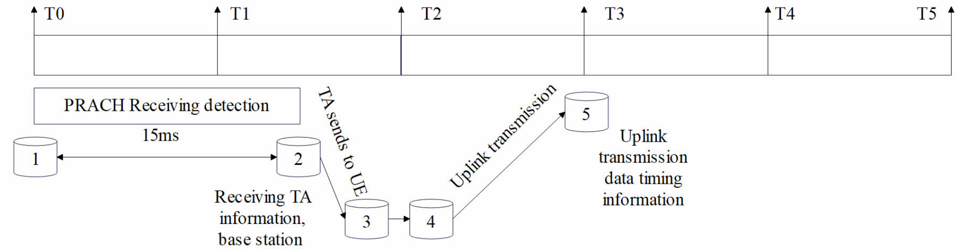
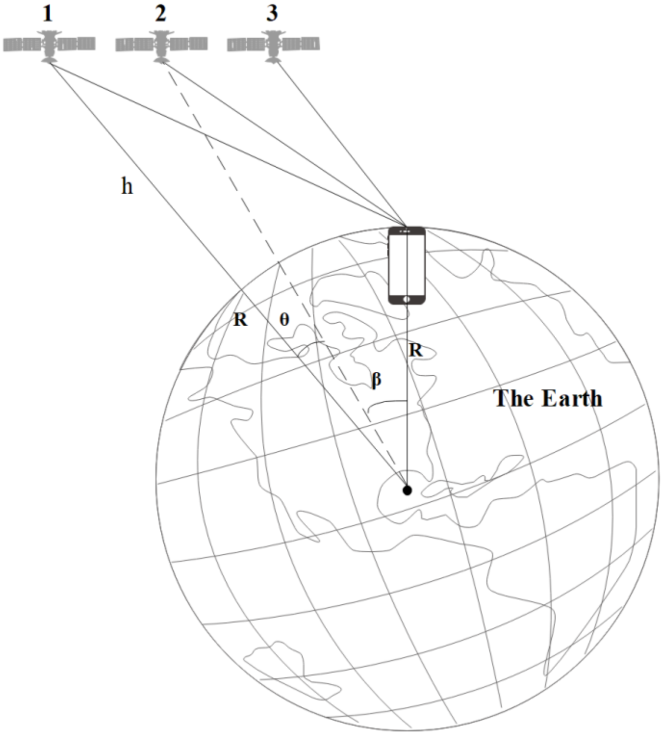

T0
T1
T2
T3
T4
T5
PRACH Receiving detection
15ms
1
2
TA sends to UE
Receiving TA information, base station
3
4
Uplink transmission
5
Uplink transmission data timing information

Figure 7 Motion trajectory during communication between satellite and UE



As shown in Figure 7, the satellite receives PRACH at position l (equivalent to time l in Figure 6), detects it, obtains TA of a certain UE, and sends it to the UE through downlink l. Then, the UE receives the TA value, adjusts it in advance, and performs uplink data transmission through the uplink 2. The satellite receives the uplink data for detection (equivalent to time 5 in Figure 6). The TA value adjusted by the user is the timing of the satellite at position 1, but the satellite performs data detection at position 2, at which time the TA has changed. The delay between position 1 and position 2 includes base station random access detection delay, downlink transmission delay, uplink adjustment TA delay, and uplink transmission delay.

The following is a specific calculation of the TA change caused by the round-trip delay. As shown in Figure 7, the radius of the earth is 6,378 km, the altitude of the satellite is h = 727 km, the largest distance of the satellite from uE is assumed to be l_1 = 1,800 km, and the speed of the satellite is v = 7.49 km/s. First, the geocentric angle of the satellite at position l is calculated, as shown in equation (8):

$$\alpha = \arccos\left(\frac{(R+h)^2 + R^2 - l_1^2}{2R(R+h)}\right) \tag{8}$$

Next, the change in the geocentric angle of the satellite from position l to position 2 is calculated, as shown in equation (9). Among them, w is the angular velocity of the satellite around the earth, and t is the time consumed by the satellite from position 1 to position 2. After the change in the geocentric angle is obtained, the geocentric angle of the satellite at position 2 [as shown in equation (10)] and the distance of the satellite from the UE at this moment [as shown in equation (11)] can be obtained.

$$\theta = wt = \frac{v}{(R+h)}t \tag{9}$$

$$\beta = \alpha - \theta \tag{10}$$

$$l_2 = \sqrt{(R+h)^2 + R^2 - 2R(R+h)\cos\beta} \tag{11}$$

Finally, it can be calculated that during the process of the satellite from position 1 to position 2, the UE needs TA to adjust the change as follows:

$$\Delta TA = 2\frac{l_1 - l_2}{c} f_s = 39.59T_s \tag{23}$$

4 Experimental study of system

4.1 Overall system design

The airborne card writing communication platform adopts a modular design method and is divided into four modules: carrier module, business module, submission dynamic library module, and message queue dynamic library module. Low coupling between modules and high cohesion within modules enhance flexibility and scalability; each module collaborates and performs its own duties, effectively improving the operational efficiency of the communication platform.

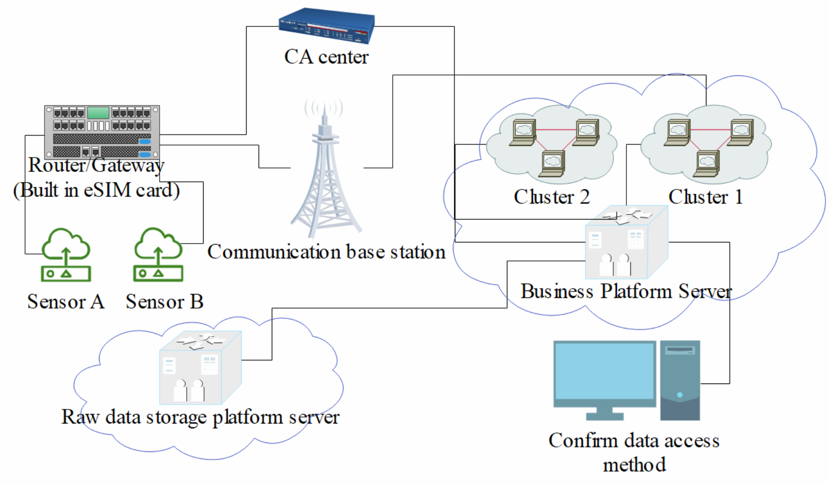
In class design, we follow the following three principles: single function principle, open/closed principle, and minimum surprise principle. The principle of single functionality means that a class should only provide a single service as a whole; the open/closed principle states that a well-designed and implemented class should be open to extensions and closed to modifications; the principle of least surprise refers to the principle that when overloading a function or implementing a parent class virtual function in a subclass, the expected functionality of the function should be maintained.

The use of streaming sockets and gateways for communication ensures the quality and stability of communication. The use of multiple processes and threads improves operational efficiency and system throughput. The use of multiplexed I/O greatly increases the concurrency of socket connections. The modular design method improves scalability and maintainability, and the configuration file method enhances program flexibility.

The eSIM card based on 5G communication can meet the needs of data traceability and tamper prevention. In addition, there is often multi-source data coordination analysis in the process of data traceability, which requires accurate determination of the source of the data. The eSIM card serves as the link between the data collection terminal side and the server side to ensure data communication and safe on-chain, thereby realising functions such as data analysis, traceability, and trusted on-chain. Figure 8 shows the architecture design of a blockchain eSIM solution based on 5G communication.

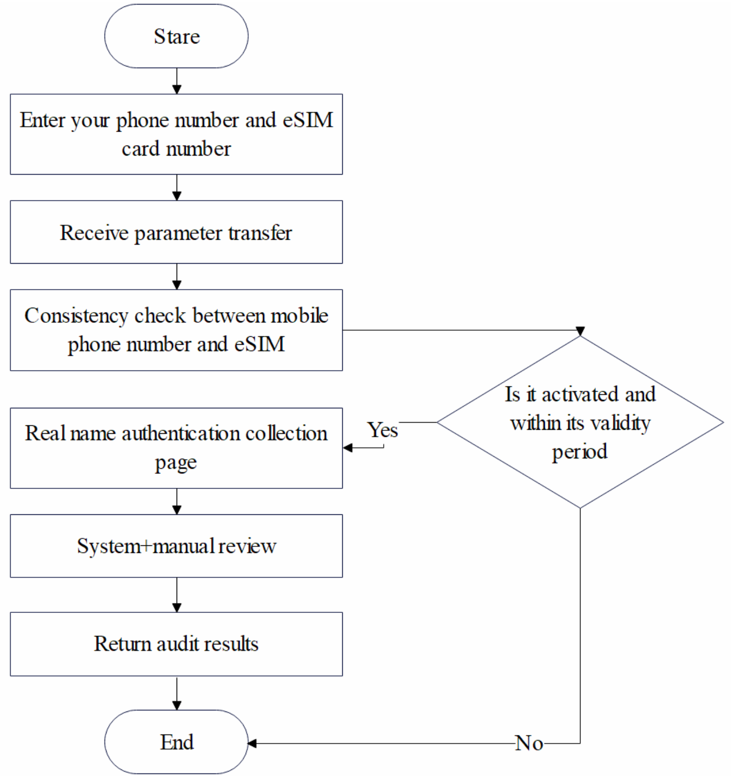
The device side composed of sensors collects data, which can be cleaned or desensitised at the edge or gateway. The built-in blockchain computing capability of eSIM card performs HASH operation on processed data. In the eSIM card operating system, the applet is placed as an application in ISD-P to implement digital signature functionality. After processing the data through the internal process of the eSIM card, signed HASH data can be obtained. Of course, for data with low sensitivity, HASH encryption operation can also be omitted and only digital signature can be performed.

Figure 8 Overall system structure diagram (see online version for colours)



There are two types of data storage. Firstly, there is on chain data storage, which stores digitally signed data processed by eSIM cards. The data will be transported by eSIM card to the nearest node of the blockchain deployed on the server side, waiting for the blockchain node to broadcast and reach consensus before being stored in the block. In addition, to verify whether the data has been maliciously tampered with, the original data will also be stored in the database in a traditional way. The reason for using two methods to store data is that the irreversibility of HASH data determines that only the original data can be compared with the data stored on the blockchain after HASH operation to determine whether the data has been tampered with.

Figure 9 Flow chart of encryption machine request


Stare
Enter your phone number and eSIM card number
Receive parameter transfer
Consistency check between mobile phone number and eSIM
Is it activated and within its validity period
Yes
Real name authentication collection page
System+manual review
Return audit results
No
End

When users perform tamper proof verification on data, they need to extract the corresponding raw data from the original database. If the blockchain stores plaintext data, they need to compare it directly. If the blockchain stores encrypted data after HASH operation, they need to perform HASH operation on the raw data and compare it with the corresponding data stored on the blockchain. Consistency means it has not been tampered with, while inconsistency means it has been tampered with.

Real-name authentication is one of the most important parts of this system. It needs to be connected to an external real-name authentication system to realise the real-name authentication of eSIM cards, that is, the real-name system for SIM cards. The real-name authentication process is shown in Figure 9.

The interface access mode is all accessed through the encryption machine introduced above. User key information is encrypted using RSA, and the interface protocol is in the form of HTTP HTTPs (encryption machine), as shown in Figure 10.

Figure 10 Docking real-name system (see online version for colours)

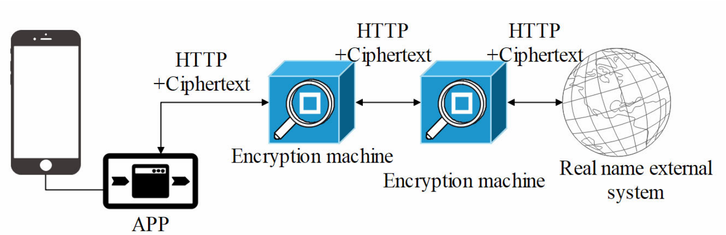
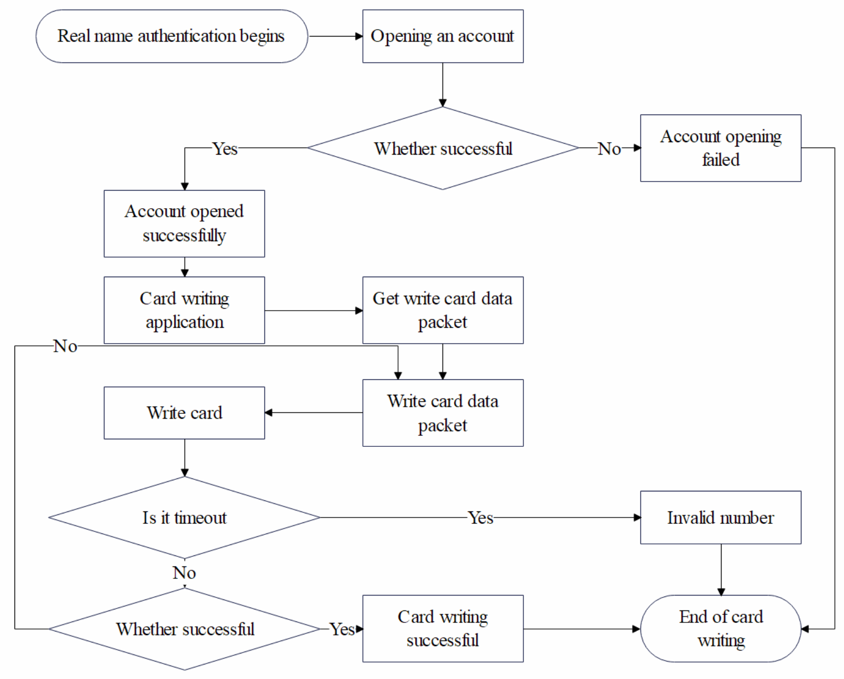


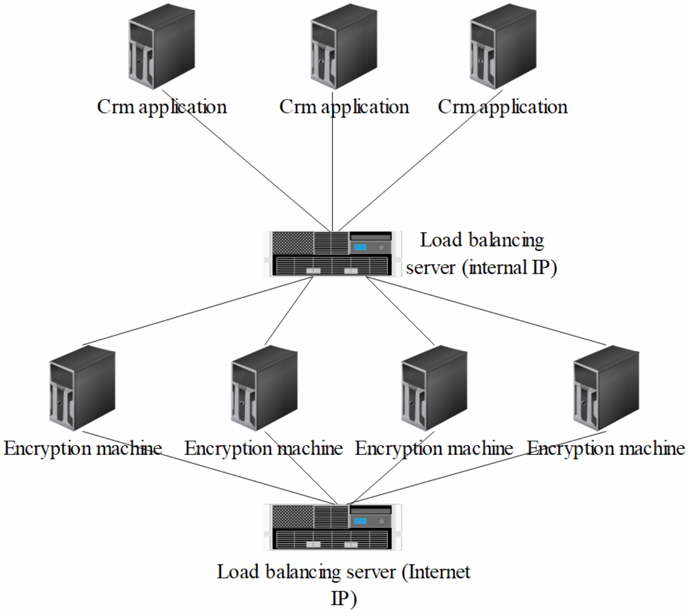
Figure 11 Flow chart of card programming and account opening



After the real-name authentication system completes the review of the submitted materials, the user returns to the APP account opening page and waits for the real-name authentication result. If the real-name authentication is successful, operations such as account opening and card programming will follow. Opening an account and obtaining card programming information are the most important links in the entire system. It needs to be connected to the mobile system to complete the entire account opening. The entire account opening and card programming flow chart is shown in Figure 11.

To connect the real-name system and the mobile system, both parties need to deploy encryption machines to ensure data security. Therefore, the first thing should be the environmental deployment of the encryption machine. The encryption machine needs to adopt the cluster deployment mode to avoid the request bottleneck problem caused by a single point of failure and a large number of concurrency. If there are too few single-node deployments or cluster instances of the access party, for the access party requesting the real-name authentication system, the access party encryption machine is at the front end of the request. Even if there are more system servers at the back end, if the front-end encryption has a request bottleneck, the request will not be transmitted to the back end. Similarly, if the access party requests the real-name authentication system, it will also cause a request bottleneck. Large concurrency means that the request cannot be sent out. Therefore, when deploying, the encryption machine needs to adopt the cluster deployment mode. The deployment topology is shown in Figure 12.

Figure 12 Deployment topology diagram (see online version for colours)



This system is a set of intelligent terminal embedded SIM card over the air card opening and real name authentication system that provides convenience for users. The system provides functions such as account opening, activation, real name authentication, recharge and payment, package management, balance inquiry, etc. for multi form terminals embedded with embedded SIM cards, and provides convenient self-service for business acceptance and inquiry for users who purchase multi form terminals with embedded SIM cards.

Random access modification scheme: in response to long delays, the random access preamble sequence has been redesigned in the physical layer with reference to ground communication systems. A polarity extension based random access sequence has been proposed to make it suitable for satellite mobile communication scenarios while maximising compatibility with ground mobile communication systems. The protocol layer has also proposed a random access response data structure that can be applied to low orbit satellite environments. Subsequently, in response to the rapid changes in TA, the physical layer proposed a downlink synchronisation tracking scheme, and the protocol layer configured reasonable parameters for the timeAligllmentTimer timer.

In the process of real name authentication and account opening, both card information and user information are very important. Therefore, in the process of calling the interface for transmission, the message information is encrypted to ensure the security of the data during transmission. Integrate with the real name authentication system and account opening system, and the key field information in the message will be encrypted with RSA in advance. However, for data security, there is also a layer of encryption machine deployed outside the server deployed in the project. That is to say, when calling the interface and transmitting data, in addition to encrypting key information, the entire message will be encrypted again. This layer of encryption machine will also be deployed at the receiving end of the real name authentication system. The encryption machine will encrypt the entire message again, and then transmit it to the encryption machine of the real name authentication system. After decryption by the other encryption machine, it will be transmitted to the internal system.

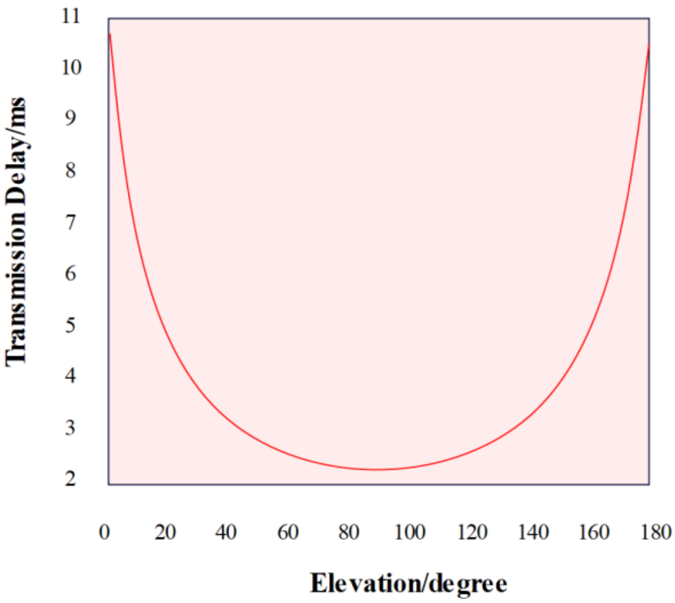
The system model in this article is constructed through embedded components, therefore it has high scalability and can be embedded in multiple terminal devices to improve the universal applicability of the model.

4.2 Results

The first is the construction of the system test environment. It is necessary to deploy the APP background system to the server, then package the APP client, and install it on the Android mobile phone for testing. The terminal is mainly Windows 7 and internet, IE8+, Firefox, Eclipse, Android Studio, Firefox, Google Chrome, etc., the server is Linux, and the database is Oracle. The hardware configuration is as follows: CPU: i9 quad-core, memory: 64 G, mobile phone: CPU: quad-core, Android system, and eSIM Watch: a mobile smartwatch configured with an eSIM card.

During one overhead of the satellite, the transmission delay changes at different elevation angles are shown in Figure 13.

Figure 13 One-way transmission delay for one overhead (see online version for colours)



This paper proposes two methods to adjust the uplink timing, one is to adjust the TA with known satellite orbit and user geographical location information, and the other is to track the uplink TA through the downlink timing change. The one-way transmission delay change rate of one overhead is shown in Figure 14.

The experiment in this paper is based on 5G communication, the base station uses band7 frequency band, the resource is 25 prb, the communication distance is 1 metre, and the speed measurement software is speedtest. The short-distance speed measurement test of the communication system is shown in Table 1.

Figure 14 One-way transmission delay rate of one overhead (see online version for colours)

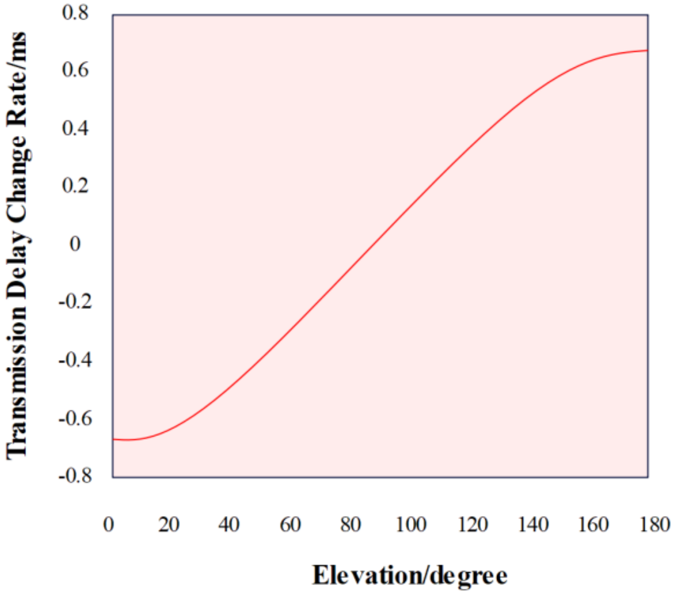


Table 1 Short-distance velocity measurement test of communication system

Number of times	*Download speed (Mbps)*	*Upload speed (Mbps)*
First time	56.03	79.50
Second time	49.70	78.71
Third time	56.63	80.39
Fourth time	51.78	78.01
Fifth time	56.93	85.64
Average speed	54.21	80.45

The base station tested this time uses the band7 frequency band, and the resource is 25 prb. The UE is placed at a different distance from the base station to test the data transmission rate. The granularity of the distance change is 1 m, and the test range is 20–100 m. The information transmission rate test at different distances is shown in Table 2.

Table 2 Velocity measurement test of communication system at different distances

High (m)	*Download speed (Mbps)*	*Upload speed (Mbps)*
20	50.688	72.072
30	45.045	51.777
40	39.798	43.362
50	30.888	38.412
60	19.305	23.166
70	11.979	14.157
80	4.455	11.979
90	2.079	9.603
100	0	0

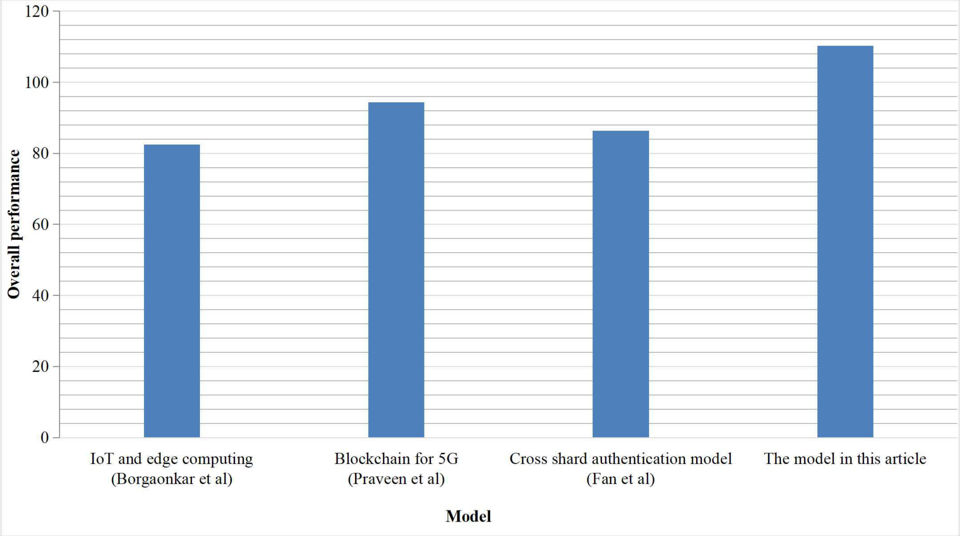
The performance test of the eSIM card is carried out through the card pass device and the module respectively. The test items and test results are shown in Table 3.

To further validate the performance of the eSIM model proposed in this paper, the model was compared with Borgaonkar et al. (2021), Praveen et al. (2020) and Fan et al. (2021), and the performance of the model was statistically analysed. The parameters in Table 3 were scored 10 points for each item, with a total score of 140 points. Based on the evaluation results of the above models, the experimental results are shown in Figure 15.

Table 3 eSIM performance test data

Test item	*Time (ms)*
Single generation key pair	575.63
Single signature task (data length 0 × 40)	472.32
Single signature task (data length 0 × 80)	506.79
Generate key pair 10,000 times (average)	660.03
Consecutive signature length 0 × 40 data 10,000 times (average)	720.75
Single read EID speed	42.77
Consecutive read EID speeds 100 times (average)	37.62
Single generation key pair	708.89
Single signature task (data length 0 × 40)	682.30
Single signature task (data length 0 × 80)	707.94
Generate key pair 10,000 times (average)	713.98
Consecutive signature length 0 × 40 data 10,000 times (mean)	756.37
Single read EID speed	87.87
Consecutive read EID speeds 100 times (average)	51.86

Figure 15 Comparison of comprehensive performance evaluation (see online version for colours)



4.3 Analysis and discussion

This system is a set of intelligent terminal embedded SIM for users to provide convenience of the over-the-air programming account opening and real-name authentication system. The system provides functions such as account opening, activation, real-name authentication, recharge and payment, package management, and balance inquiry for multi-form terminals embedded with China Mobile's embedded SIM card. Moreover, it provides convenient self-service of service acceptance and inquiry for users who have purchased multi-form terminals with built-in embedded SIM. The system is mainly divided into three major systems. Among them, one is to establish a connection communication between the eSIM watch and the mobile APP through Bluetooth, and then perform data interaction. The second is the development of eSIM mobile APP. The third is that the mobile APP connects with three external interface platforms: real-name authentication online company, mobile company, and capability development platform. After the online company is successfully registered with the real name, the system calls the interface of the mobile company to obtain the card programming information. After obtaining the card programming information, the card programming information is saved to the background database and transmitted to the APP side. After the APP side obtains the card programming information, the card programming information is transmitted to the watch to start programming the card. At this time, no matter whether the card programming is successful or failed, the watch will return a card programming result to inform the APP side, and then the APP side calls the mobile company interface to inform the mobile company of the card programming result, and the entire over-the-air programming is completed.

As shown in Figure 13, the abscissa is the elevation angle of the user on the ground in degrees. The ordinate is the one-way transmission delay from the satellite to the ground, and the unit is ms. When the elevation angle is 90°, the satellite is over the top. At this moment, the distance between the user and the satellite is the shortest, and the shortest one-way transmission delay is 2.42 ms. The longest communication distance between the satellite and the user is 1,800 km, the longest one-way transmission delay is 6 ms, and the elevation angle at this time is about 17° and 163°. Due to the rapid movement of the satellite, the timing in the uplink transmission process is constantly changing, so it is necessary to take effective measures to track the uplink timing and constantly adjust it.

The principle of TA adjustment based on known satellite orbit and user location information is that the satellite orbit and orbiting speed are known, so the position of the satellite at any time can be calculated. The user can obtain his own geographical location information through the global positioning system, so when the user obtains the satellite orbit information, he can calculate the distance between himself and the satellite at any time according to his own geographical location information, and after knowing the distance between the two, he can calculate the amount of timing and advance required for uploading data, so that there is no need for frequent TA adjustments.

Short distance communication data transmission plays an important role in verifying the system communication speed. This article verifies the short distance communication transmission effect of the model. The verification is mainly divided into two items: upload speed and download speed, and the speed directly reflects the performance. As shown in Table 1, the short-distance network speed of the OAI communication system is relatively fast. The download speed of the first speed measurement can reach 56.03 Mbps, and the upload speed can reach 79.5 Mbps. After 5 times of speed measurement, the average download speed of information can reach 54.21 Mbps, and the average upload speed can reach 80.45 Mbps. The speed measurement at different times is relatively stable.

The UE used in this test is a computer plugged into an internet access card. The base station uses band7 frequency band with a resource of 25 prb. The UE is placed at a different distance from the base station to test the data transmission rate. The granularity of the distance change is 1 m, and the testing range is 1–15 m, as shown in Table 2, a big problem in the OAI communication system is that the short-distance communication effect is relatively good, but as the distance between the UE and the base station becomes farther, the communication transmission rate drops sharply. When the distance reaches 100 m, the communication between the two is unable to communicate. Another problem is that the support for mobility is relatively poor. During the test, if the UE moves a little faster after accessing the internet, the connection is likely to be interrupted. At this time, the connection with the base station needs to be reestablished.

As shown in Table 3, the performance test results of the over-the-air programming and real-name authentication technology based on 5G communication proposed in this paper performed well. It can be seen that the over-the-air programming and real-name authentication technology of eSIM based on 5G communication technology proposed in this paper has certain effect.

From Figure 15, it can be seen that the comprehensive performance of the model in this article is higher than that of models in recent years. Combining with the model in this article, it can play an important role in 5G communication technology and effectively improve the comprehensive performance of 5G communication models.

Orbital satellite mobile communication uses a protocol stack based on ground communication. The existing ground communication protocol stack is relatively mature and stable in operation, but it is designed based on the application scenarios of ground objects, suitable for object movement speeds less than the speed of high-speed trains, and the coverage distance of one base station does not exceed 100 kilometres. However, the movement speed of low orbit satellite mobile communication systems far exceeds that of ground objects, and the distance covered by satellites also exceeds 100 kilometres. The model proposed in this article is suitable for short-range ground transmission needs, especially in the field of vehicle networking and other important applications. It can play an important role in the field of vehicle networking and effectively improve the data transmission efficiency in these areas.

5 Conclusions

With the rapid development of the IoT, more and more smart terminal devices will use eSIM cards, mainly including smart watches, vehicle equipment, drones, wearable devices, etc. These IoT devices usually work in complex and harsh environments. Because these IoT devices usually work in complex and harsh environments, traditional SIM cards obviously cannot meet the communication requirements of these IoT devices, and the use of eSIM cards has become the first choice. In this paper, a new random access design is proposed for the long delay and rapid TA changes of the LEO satellite communication system. The new design requires the transformation of the protocol layer and the physical layer. At the physical layer, a random access preamble structure based on polarity expansion and a new TA adjustment strategy based on downlink tracking are proposed. In the protocol layer, the data structure of random access response is designed, which is suitable for LEO satellite environment. These modifications enable the communication system to adapt to the characteristics of long delay and rapid change of TA in satellite transmission scenarios, and at the same time ensure the compatibility with ground systems to the greatest extent. Moreover, this paper verifies the effectiveness of the proposed technology combined with experimental tests. In addition, the number of users supported by the original system is limited, so it is necessary to further optimise the code to enable the communication system to access more users, which is also the follow-up research direction.

The model in this article is limited by conditions and has not been tested in large-scale practical environments. Therefore, further experimental research is needed in combination with the algorithm model in this article to improve the practical effectiveness of the model.

References

Abdel Hakeem, S.A., Hady, A.A. and Kim, H. (2020) 'Current and future developments to improve 5G-NewRadio performance in vehicle-to-everything communications', *Telecommunication Systems*, Vol. 75, No. 3, pp.331–353.

Apilo, O., Karhula, P. and Mäkelä, J. (2022) 'eSIM-based inter-operator mobility for advanced smart products', *IEEE Internet of Things Magazine*, Vol. 5, No. 2, pp.120–126.

Borgaonkar, R., Tøndel, I.A., Degefa, M.Z. and Jaatun, M.G. (2021) 'Improving smart grid security through 5G enabled IoT and edge computing', *Concurrency and Computation: Practice and Experience*, Vol. 33, No. 18, pp.e6466–e6475.

Casetti, C. (2022) 'The lively versatility of the 5G Ecosystem [mobile radio]', *IEEE Vehicular Technology Magazine*, Vol. 17, No. 2, pp.4–13.

Demirev, V. (2020) 'World Radio Communication Conference WRC '19 – impact over security of the modern human society', *Security & Future*, Vol. 4, No. 2, pp.72–74.

Dymkova, S. (2021) 'Applicability of 5G subscriber equipment and global navigation satellite systems', *Synchroinfo Journal*, Vol. 7, No. 5, pp.36–48.

Fan, C.I., Shih, Y.T., Huang, J.J. and Chiu, W.R. (2021) 'Cross-network-slice authentication scheme for the 5th generation mobile communication system', *IEEE Transactions on Network and Service Management*, Vol. 18, No. 1, pp.701–712.

He, W., Xu, B., Scialacqua, L., Ying, Z., Scannavini, A., Foged, L.J., … and He, S. (2021) 'Fast power density assessment of 5G mobile handset using equivalent currents method', *IEEE Transactions on Antennas and Propagation*, Vol. 69, No. 10, pp.6857–6869.

Ibarrola, E., Jakobs, K., Sherif, M.H. and Sparrell, D. (2023) 'The evolution of telecom business, economy, policies and regulations', *IEEE Communications Magazine*, Vol. 61, No. 7, pp.16–17.

Khalid, A., Rashid, F., Tahir, U., Asif, H.M. and Al-Turjman, F. (2022) 'Multi-carrier visible light communication system using enhanced sub-carrier index modulation and discrete wavelet transform', *Wireless Personal Communications*, Vol. 127, No. 1, pp.187–215.

Kim, H.K., Cho, Y. and Jo, H.S. (2020) 'Adjacent channel compatibility evaluation and interference mitigation technique between earth station in motion and IMT-2020', *IEEE Access*, Vol. 8, No. 5, pp.213185–213205.

Lin, X., Cioni, S., Charbit, G., Chuberre, N., Hellsten, S. and Boutillon, J.F. (2021) 'On the path to 6G: embracing the next wave of low Earth orbit satellite access', *IEEE Communications Magazine*, Vol. 59, No. 12, pp.36–42.

Luglio, M., Quadrini, M., Roseti, C. and Zampognaro, F. (2022) 'Modes and models for satellite integration in 5G networks', *IEEE Communications Magazine*, Vol. 61, No. 4, pp.50–56.

Mao, W., Zhao, Z., Chang, Z., Min, G. and Gao, W. (2021) 'Energy-efficient industrial internet of things: overview and open issues', *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 11, pp.7225–7237.

Medeiros, H.D.S., Bezerra, L.d.S., España, F.T. and de Oliveira, J.T.S. (2024) 'Embedded-SIM (e-SIM) an overview in Latin America: implementation, availability, advantages and disadvantages', *Journal of Communication and Information Systems*, Vol. 39, No. 1, pp.46–57.

Mishra, L., Vikash, S. and Varma, S. (2021) 'Seamless health monitoring using 5G NR for internet of medical things', *Wireless Personal Communications*, Vol. 120, No. 3, pp.2259–2289.

Praveen, G., Chamola, V., Hassija, V. and Kumar, N. (2020) 'Blockchain for 5G: a prelude to future telecommunication', *IEEE Network*, Vol. 34, No. 6, pp.106–113.

Su, Y. (2021) 'A trust based scheme to protect 5G UAV communication networks', *IEEE Open Journal of the Computer Society*, Vol. 2, No. 3, pp.300–307.

Suomalainen, J., Julku, J., Vehkaperä, M. and Posti, H. (2021) 'Securing public safety communications on commercial and tactical 5G networks: a survey and future research directions', *IEEE Open Journal of the Communications Society*, Vol. 2, No. 1, pp.1590–1615.

Tusha, S.D., Tusha, A., Basar, E. and Arslan, H. (2020) 'Multidimensional index modulation for 5G and beyond wireless networks', *Proceedings of the IEEE*, Vol. 109, No. 2, pp.170–199.

Vikhrova, O., Pizzi, S., Terzani, A., Araujo, L., Orsino, A. and Araniti, G. (2022) 'Multi-sim support in 5G evolution: challenges and opportunities', *IEEE Communications Standards Magazine*, Vol. 6, No. 2, pp.64–70.