A security transmission system for Beidou short message based on SM9

Ruiyun Hu¹, Lei Ju² and Pengyu Chen¹*

¹ Department of Electronics and Communication Engineering, Beijing Electronic Science & Technology Institute, Fengtai, Beijing, 100070, China
²Department of Electronics and Communication Engineering, Beijing Electronic Science & Technology Institute, Fengtai, Beijing, 100070, China
*Corresponding author’s e-mail: 18513105080@163.com

Abstract. With the increasing application of Beidou communication technology, the safety of the short message communication process of Beidou satellite navigation system becomes more and more important. Direct communication with Beidou short messages lacks reliable data security protection measures. In order to transmit Beidou short message safely and reliably, according to the characteristics of Beidou short message protocol and message structure, this paper proposes a security transmission system for Beidou short message based on sm9, which can meet the security requirements of the communication, and the cost investment is also greatly reduced.

1. Introduction
Beidou Satellite Navigation System (BDS) is a global satellite navigation system and communication system developed by China [1], providing rapid positioning, real-time navigation, precise timing, location reporting, short message service and other services for military and civilian users, with the advantage of safety and reliability [2]. The Beidou short message is a special feature of the Beidou satellite navigation system, which is different from other major navigation and positioning systems in the world. Beidou short message has the advantages of wide coverage, short construction period and low investment cost. It has been widely used in many industries such as intelligent transportation, forest fire prevention, agricultural intensive cultivation, power monitoring and hydrological monitoring. Therefore, it is necessary to design a suitable security protection scheme for Beidou short message to ensure that sensitive data can be transmitted securely through Beidou short messages.

2. Related work
Beidou satellite communication refers to the use of Beidou navigation satellite as a relay station to forward radio waves and communicate between two or more earth stations. It is an emerging wireless communication technology developed on the basis of microwave communication and aerospace technology. The radio wave frequency used is the microwave frequency band (300 MHz to 300 GHz, that is, the band 1 m to 1 mm). Such a communication system that uses Beidou navigation satellites to communicate between earth stations is called a Beidou satellite communication system [3-4].

The Beidou communication network is a space-based wireless communication network based on the Beidou satellite navigation system. The transmission unit of the network is a short message under the Beidou communication protocol [5]. The biggest feature of Beidou system is its active positioning and
short message service. It not only solves the problem of satellite navigation system in China, but also combines SMS and navigation. It is a unique invention of China Beidou satellite navigation system and a major advantage [6]. Beidou short message has some limitations from the application point of view:

1) Communication capacity limitation. With short message communication, one communication has a capacity limitation, that is, the length of each communication content is limited. Under normal circumstances, the maximum capacity of each short message of civil communication is 78 bytes [7].

2) Communication frequency limitation. When Beidou is in use, it has requirements for frequency. The general frequency of use of the device is basically 1 min, that is, it can be used once for 1 min. If more high frequency is required, a special application is required when entering the network [8].

3) Communication is not reliable. The Beidou satellite communication link is an unreliable communication link, and the Beidou civil communication system has no communication receipt.

In order to transmit Beidou short message communication data safely and reliably, according to the characteristics of Beidou short message protocol and message structure, this paper proposes a safe transmission scheme of Beidou short message based on SM9, which can meet the security requirements of device communication, and also reduces the complexity of certificate management, key exchange and key management, and greatly reduces the cost investment.

3. System description

3.1. framework design

Figure 1 shows the overall framework of encryption and decryption of the Beidou short message communication system. The Beidou antenna enhances signal transmission and signal reception. The Beidou communication module is integrated inside the GNSS.

The Beidou communication module of the data sender performs signature processing and encryption on the received Beidou short message communication data. The data receiver Beidou communication module performs the verification processing and decryption of the received Beidou short message communication data.
3.2. Key registration module

The device connects to the key generation center (KGC), submits its pre-assigned identity ID, applies the private key of the SM9 algorithm, and injects the private key into the device in a secure manner. As shown in figure 2.

3.3. Identification cryptosystem based on SM9

The identity-based cryptography was first proposed by Shamir in 1984. In this system, the public key is the identity information of the user, such as the IP address of the host, the user's E-mail address, mobile phone number and name. The private key is generated by the KGC (Key Generation Centre) based on the identity information of the user, and the private key is sent to the corresponding user through the secure channel. Because the user's public key is directly calculated from the identity information, there is no need to store the public key or certificate in the process of using the public key, and no CA (third party) is required to provide the service.

SM9 is an identity-based public key system. The two parties can calculate the other party's public key based on each other's identity ID, thus reducing the complexity of key exchange and key management. Therefore, the security protection method based on the identity-based cryptosystem can not only meet the authentication security requirements of substation communication, but also reduce the complexity of certificate management.

3.4. SM9 encryption and decryption mechanism

Figure 3. SM9 encryption and decryption mechanism.
As shown in figure 3, the SM9 algorithm is used to encrypt and decrypt important data to ensure the confidentiality and integrity of the data during the communication process. In the SM9 identification cipher algorithm, the user's public key is derived from identity information, and the private key is generated by KGC. As long as the identity information of the user is obtained, the user B can obtain the public key of the user A, and encrypt the message with the public key of the user A, so that it is securely transmitted to the user A in the form of ciphertext on the network, and the user A is from the SM9. After obtaining the private key of the key center, the message can be decrypted, thereby realizing encryption and decryption of data transmission between the terminal and the platform.

4. Test Results

4.1. Unencrypted data test results

After receiving the Beidou short message communication data, the GNSS receiver sends the Beidou short message communication data plaintext to the RS232 serial port, and the RS232 serial port outputs the Beidou short message communication data plaintext to the user PC serial debugging assistant. As shown in Figure 4.

![Figure 4. Unencrypted data test results.](image)

4.2. Encrypted data test results

After receiving the Beidou short message communication data, the GNSS receiver encrypts by using the SM9 algorithm, and then outputs the encrypted Beidou short message communication data to the serial debugging assistant of the user PC through the RS232 serial port, as shown in Figure 5. The encrypted Beidou short message communication data is a string of garbled characters.

![Figure 5. Encrypted data test results.](image)

4.3. Encryption and decryption communication data test verification

After receiving the Beidou short message communication data, the GNSS receiver uses the SM9 algorithm to encrypt, and then outputs the encrypted Beidou short message communication data to the user PC serial debugging assistant through the RS232 serial port. Decryption processing is performed, and the Beidou short message communication data is transmitted to the serial port debugging assistant, and the obtained encrypted data and decrypted data are as shown in Figure 6.

![Figure 6. Encryption and decryption communication data test verification.](image)

5. Conclusion

At present, the Beidou short message lacks reliable data security protection measures. According to the transmission mechanism of Beidou communication system and the knowledge of cryptography, this paper designs and implements the use of SM9 algorithm to encrypt and decrypt the Beidou short
message, and tests and verifies it in the serial debugging device. The result shows that the mechanism can ensure the safe transmission of data.

References
[1] TANG J, YU L, WANG S. Applying Current Situation Analysis of Beidou Satellites Navigation Positioning System [J]. Gnss World of China, 2008, 2.
[2] WANG X, YIN Y, YANG Z. Modernization Progress of Global Navigation Satellite Systems [J]. Gnss World of China, 2006, 4.
[3] Chen S, Xu H, Liu D, et al. A vision of IoT: Applications, challenges, and opportunities with china perspective[J]. IEEE Internet of Things journal, 2014, 1(4): 349-359.
[4] Xinfei B A, Wang P. Design of soldier status monitoring and command and control system based on Beidou system[C]//Proceedings of 2012 2nd International Conference on Computer Science and Network Technology. IEEE, 2012: 1362-1366.
[5] Zhou W, Hou J, Fan W, et al. A location-based marine fishery information service based on BeiDou navigation satellite system[J]. Journal of Intelligent & Fuzzy Systems (Preprint): 1-8.
[6] Gong M F, Wang Z G, Xiao H Y, et al. Application of Beidou Short Message Communication in Meter Reading System[J]. Automation & Instrumentation, 2015 (7): 9.
[7] Yang Y, Xu Y, Li J, et al. Progress and performance evaluation of BeiDou global navigation satellite system: Data analysis based on BDS-3 demonstration system[J]. Science China Earth Sciences, 2018, 61(5): 614-624.
[8] Hao M, Zhang J, Niu R, et al. Application of BeiDou navigation satellite system in emergency rescue of natural hazards: a case study for field geological survey of Qinghai–Tibet plateau[J]. Geo-spatial Information Science, 2018, 21(4): 294-301.