micromachines

Article

Data and Service Security of GNSS Sensors Integrated with Cryptographic Module

Changhui Xu [1,2,*], Jingkui Zhang [1], Zhiyou Zhang [3], Jianning Hou [4] and Xujie Wen [4]

[1] State Key Laboratory of Satellite Navigation System and Equipment Technology, Shijiazhuang 050081, China
[2] Key Laboratory of Surveying and Mapping Science and Geospatial Information Technology of MNR, Chinese Academy of Surveying & Mapping, Beijing 100036, China
[3] Geology Surveying and Mapping Institute of Guangdong, Guangzhou 510800, China
[4] National Engineering Research Center of Cryptography Science and Technology, Beijing 100043, China
* Correspondence: chxu@casm.ac.cn

Abstract: Navigation and positioning are of increasing importance because they are becoming a new form of infrastructure. To ensure both development and security, this study designed a technical innovation structure to upgrade the GNSS (Global Navigation Satellite System) data transmission and real-time differential correction service system and proposed a new multiple cryptographic fusion algorithm to achieve the encryption and decryption of GNSS data and services. First, a GNSS station encrypts GNSS data with an encryption key and obtains a public key from a GNSS data center to encrypt the GNSS data encryption key. After that, identity authentication of a GNSS station is carried out, and an SSL VPN is established between the GNSS station and a GNSS data center before GNSS data are transmitted to the GNSS data center. Then, the GNSS data center decrypts the received GNSS data. The process of an intelligent terminal for real-time differential corrections is similar to that of the GNSS station and the GNSS data center. A GNSS sensor integrated with a cryptographic module was developed to validate the structure in an open environment. The results showed that the developed GNSS sensor was successful in encrypting the data, and the GNSS data center was able to decrypt the data correctly. For the performance test, a cryptography server was able support the requirements of GNSS applications. However, a cryptography server was optimal in supporting 40~50 GNSS stations simultaneously, whereas a cluster was suggested to be configured if the number of GNSS stations was more than 60. In conclusion, the method was able to ensure the validity, confidentiality, integrity, and non-repudiation of GNSS data and services. The proposed upgrading technology was suitable for coordinating GNSS development and security.

Keywords: GNSS; cryptography; data security; service security; integrity protection; authorization; confidentiality

check for updates

Citation: Xu, C.; Zhang, J.; Zhang, Z.; Hou, J.; Wen, X. Data and Service Security of GNSS Sensors Integrated with Cryptographic Module. *Micromachines* **2023**, *14*, 454. https://doi.org/10.3390/mi14020454

Academic Editors: Huafeng Liu, Yuan Wang and Stefano Mariani

Received: 15 November 2022
Revised: 10 February 2023
Accepted: 13 February 2023
Published: 15 February 2023

1. Introduction

Surveying and mapping geographical information are important parts of national basic data, the security of which is a matter of national security. Generally, this information includes three types of data. Secret data are used for secret-related people, public data are used for every person, and controlled data between these two types of data are used for private people. Global navigation satellite system (GNSS) reference stations (also named Continuously Operating Reference Station, CORS) are the key infrastructure of surveying and mapping geographical information for high-precision navigation and positioning concerning these three types of data and are thus paid more attention. GNSS reference stations are the fixed stations on the ground that receive long-term continuous measured satellite signals; they transmit to the data center, in real time or at regular times, via communication facilities. Besides GNSS reference stations, GNSS receivers are applied for deformation monitoring, including landslide monitoring, oil rig monitoring, bridge monitoring, and high precision location services, including intelligent terminals, wearable devices, and special vehicles. Traditionally, we only pay attention to GNSS reference stations, the data of which are transmitted by private networks for security. However, the security of GNSS monitoring stations is not focused on because they are generally distributed over a small area. With the increasing importance of data security and individual privacy, applications of GNSS receivers should be controlled; otherwise, they will cause security hazards.

GNSS monitoring data for landslides, bridges, and oil rigs are transmitted on the internet, by tradition. Landslide monitoring usually sets several GNSS monitoring stations on a side slope or geological hazard susceptibility slope to obtain GNSS observations for deformation and sedimentation monitoring [1,2]. Bridge monitoring uses three to more than ten stations on different parts of a bridge to monitor its dynamic deformation and extract its structural health characteristics [3,4]. Oil rig monitoring also uses several GNSS stations to analyze a platform's shaking trend and structural characteristics for offshore platform security [5–7]. The risk of these data is small, because the monitoring stations are usually distributed over a limited area. However, with the development of the internet, big data, and artificial intelligence, if GNSS monitoring data in a large area, even nationwide, are illegally collected, these data can be used to analyze national unstable regions, which can cause military or other risks.

GNSS high-precision location services are widely used for various fields. To obtain the high-precision coordinates, there are two main modes. One is Precise Point Positioning (PPP), which uses station observations to obtain the centimeter-level coordinates of the station with global precise orbit and clock corrections [8–10]. The other mode is Real Time Kinematic (RTK), or network RTK, which uses a reference station or reference network stations to eliminate common errors between a solution station and the reference stations so that real-time centimeter-level coordinates can be determined [11]. However, PPP has a long convergence, and RTK is limited by the distance between a rover station and a reference station. To optimize the advantages and complement the disadvantages of PPP and RTK, PPP-RTK has been developed, which can obtain centimeter-level coordinates without a reference station [12–15]. Therefore, GNSSs are increasing for location-based services, natural source surveying and monitoring, and intelligent terminals because of their high precision. Especially, with the ability of GNSS observations' output in mobile phones, high-precision positioning of mobile phones is rapidly being investigated to provide precision positioning for the public [16,17]. All researchers focus on how to obtain high-precision positioning, and the techniques and applications have made great improvements. However, the security of GNSS data and service is not paid close attention. High-precision positions, especially individual and special vehicle trajectories, are private, which may cause personal risks, such as using individual information for illegal actions. It is necessary to develop a new method to protect information when these applications are popularized.

To improve the GNSS data security, there are mainly two types of solutions. One solution is based on algorithms. The multi-constellation receiver has better counter spoofing and replaying attacks, an approach of the clustering-based solution separation algorithm which was developed with the advantage of more redundant measurements [18]. By validating absolute and relative times of cross-checking the GNSS time, and time from other available sources, a time offset validation method is proposed to detect if the GNSS receiver was attacked or not [19]. The other solution for GNSS protection is cryptography. Panagiotis (2008) put forward the fusion of cryptography and GNSS in the future [20], and his team conducted some research about the analysis of attacks and countermeasures on cryptographically protected or unprotected GNSS signals [20,21]. At the same time, some studies are on the way, such as cryptographic authentication of the GPS navigation message, spoofing attacks against cryptographically secured GNSS signals of a hypothesis test, and cryptographic integrity of the navigation message [22–24]. A type of GNSS reference station (P5E) of CHC Navigation supports the HTTPs encryption. This study focused on security of GNSS data transmission from a receiver to a data center and a real-time differential correction service. We design a whole protection framework of GNSS data transmission and a real-time differential service with the cryptography technique to ensure the validity, confidentiality, integrity, and non-repudiation of GNSS data and services. At the same time, we improved a fusion algorithm based on multiple cryptographic algorithms for protection of the data source, encryption key, and transmission. Moreover, we also develop a new GNSS receiver integrated with a cryptographic module and validate the feasibility with an open environment.

2. Security Risk Nodes of GNSS Data and Service

Observation and navigation files of GNSS stations are free to download with a time delay by ftp or http in some countries of the world. At the same time, the International GNSS service (IGS) also provides the real-time service (RTS) correction streams for free to the broadcast ephemeris after registration. However, some information about GNSS reference stations is controlled for use in China to improve GNSS data security. This information includes four nodes from GNSS observation transmission to service, as shown in Figure 1.

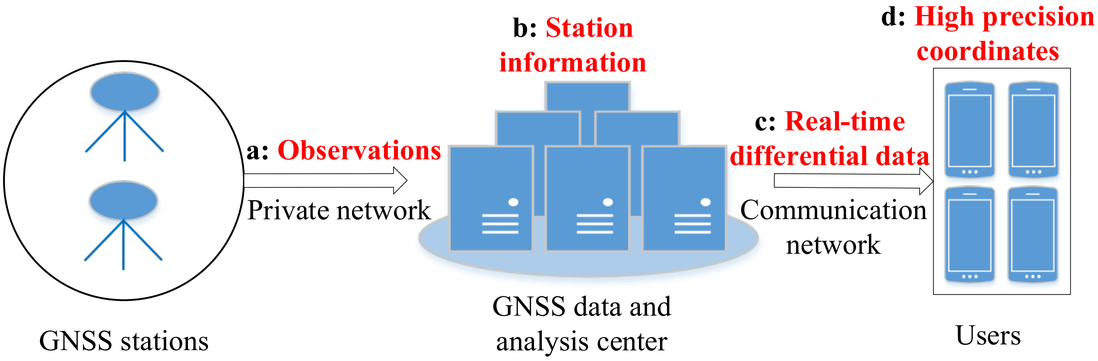

Figure 1. Security hazard nodes of GNSS data transmission and service.

a. A GNSS receiver receives signals from GNSS satellites and transmits them to the GNSS data center. These signals can be transformed into GNSS observations such as pseudorange, carrier phase, and Doppler shift, which are controlled for use.
b. Some GNSS CORS station information is controlled, except the secret data of original reference station coordinates and reference station network observations. This CORS station information is mainly the station name, type, level, location, receiver type, and so on.
c. Real-time differential data are for two types of service. RTS combination products consisting of GNSS satellite orbit and clock corrections are for precise point positioning and real-time correction data for RTK or network RTK.
d. All controlled data are used after verification and registration. Especially, service better than 1 m accuracy is in a higher controlled level.

3. Upgrading Structure of GNSS Integrated with Commercial Cryptography

It is of great significance to use commercial cryptography for presenting security hazards, so that the data are protected from stealing and tampering. To improve the security protection, we have to construct a basic commercial cryptography infrastructure, which consists of a cooperative signature system, digital certification identification system, key management system, cryptography management system, cryptography server, and a virtual private networks (VPN) server. The commercial cryptography infrastructure provides data encryption, data decryption, identical authentication, a virtual channel for data transmission, integrity protection, a collaborative signature, and key management for GNSS data transmission, storage, and service.

For the support of the commercial cryptography infrastructure, we proposed a plan of GNSS data security protection, as shown in Figure 2. The plan included the whole chain of

GNSS data transmission, processing, storage, and a real-time differential correction service. In the process of GNSS data transmission from a GNSS receiver to a GNSS data center, the identification of the GNSS data center is authorized, the GNSS data are encrypted, and a virtual channel of GNSS data transmission is established. When the GNSS data are valued and stored, the signature is verified first, and then the GNSS data center is decrypted for usage and encrypted again for storage. At the same time, data integrity and the system log are protected.

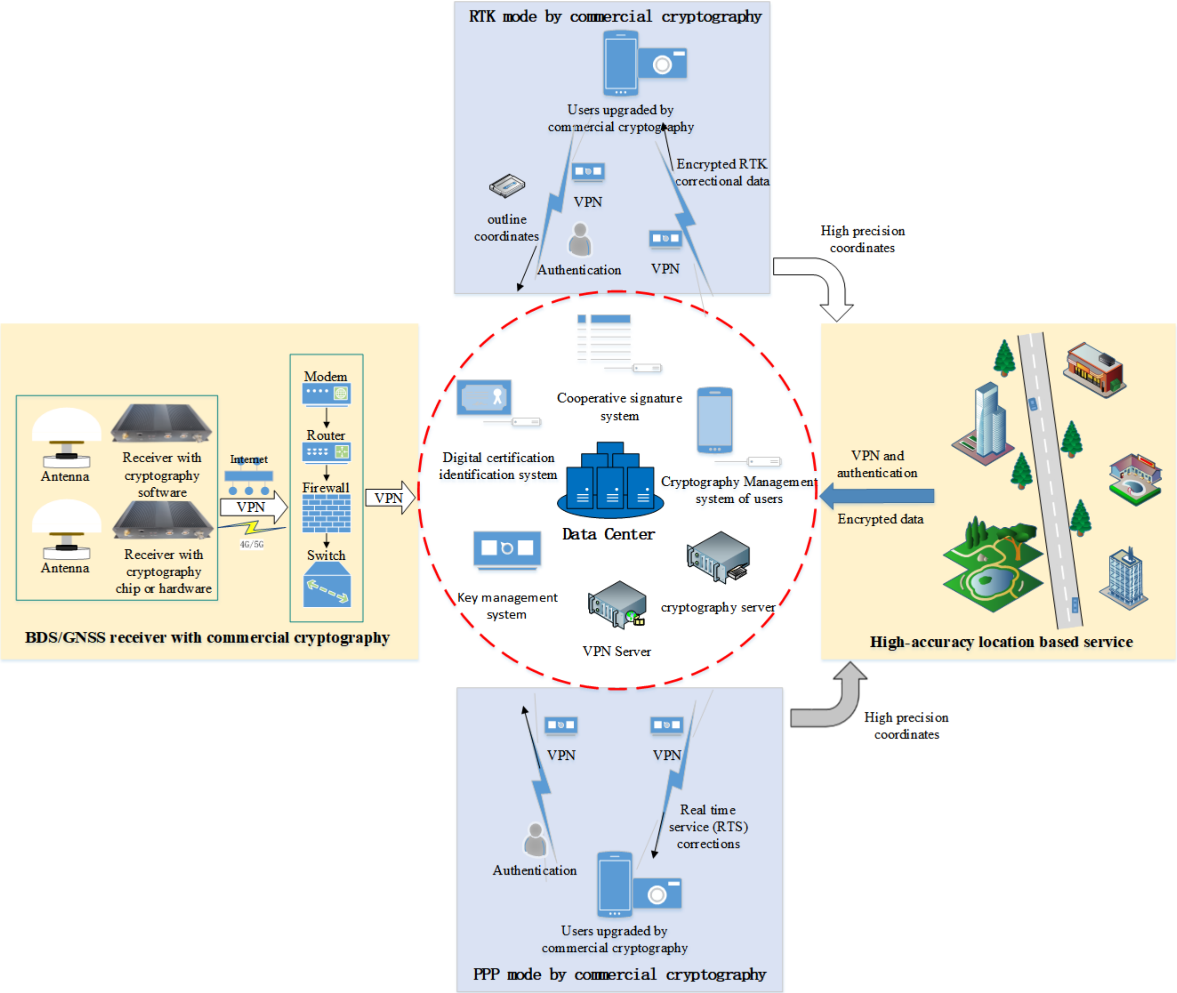
RTK mode by commercial cryptography
Users upgraded by commercial cryptography
Encrypted RTK correctional data
VPN
outline coordinates
Authentication
VPN
High precision coordinates
Modem
Router
Firewall
Switch
Antenna
Receiver with cryptography software
Internet
VPN
4G/5G
Antenna
Receiver with cryptography chip or hardware
VPN
BDS/GNSS receiver with commercial cryptography
Cooperative signature system
Digital certification identification system
Cryptography Management system of users
Data Center
Key management system
cryptography server
VPN Server
VPN and authentication
Encrypted data
High-accuracy location based service
High precision coordinates
VPN
VPN
Real time service (RTS) corrections
Authentication
Users upgraded by commercial cryptography
PPP mode by commercial cryptography

Figure 2. Commercial cryptography updating plan.

There are two types of service modes for high precision positioning to increase the GNSS data value. PPP can reach centimeter positioning precision using the RTS combination products with convergence over a period of time. RTK or network RTK uses correctional data of a single station or regional stations to obtain centimeter positioning precision within a minute. Therefore, we proposed two different commercial cryptography updating plans for these two application modes. A virtual channel and the authentication and integrity of PPP are required, while RTK needs a data encryption besides a virtual channel, authentication, and integrity. When we receive the high-precision coordinates of a position with these modes, they will become the controlled information if the coordinates are higher than some level or combined with geographic attribute information. This information is not suitable to transmit directly by a network. However, it is transmitted by the network after the commercial cryptography updating of security, integrity, and the virtual channel.

4. GNSS Data Security Protection Integrating Multiple Cryptographic Algorithms

Domestic commercial cryptography has many encryption algorithms, such as SM2, SM3, SM4, and SM9. The combination of SM2 and SM4 is used for the GNSS data security protection, where SM4 is to encrypt the GNSS RTCM data and SM2 is to encrypt the encryption key.

GNSS RTCM data encryption uses an SM4 algorithm that encrypts and decrypts GNSS RTCM data with the same key so that it has high efficiency and fast encryption and decryption, with low costs and resources. However, the disadvantages of SM4 are the transmission, storage, and management of the cipher. To improve the security of the SM4 cipher, truly random numbers are generated regularly as the GNSS RTCM data encryption key by the cryptographic module. The SM4 algorithm is a block encryption algorithm with a block length and key length of 128 bits. It uses a nonlinear iterative structure of 32 rounds operated by nonequilibrium Feistel, with the same algorithm structure for encryption and decryption, and is easy to implement in hardware because of the same circuit topology. The iterative encryption algorithm is given in Figure 3.

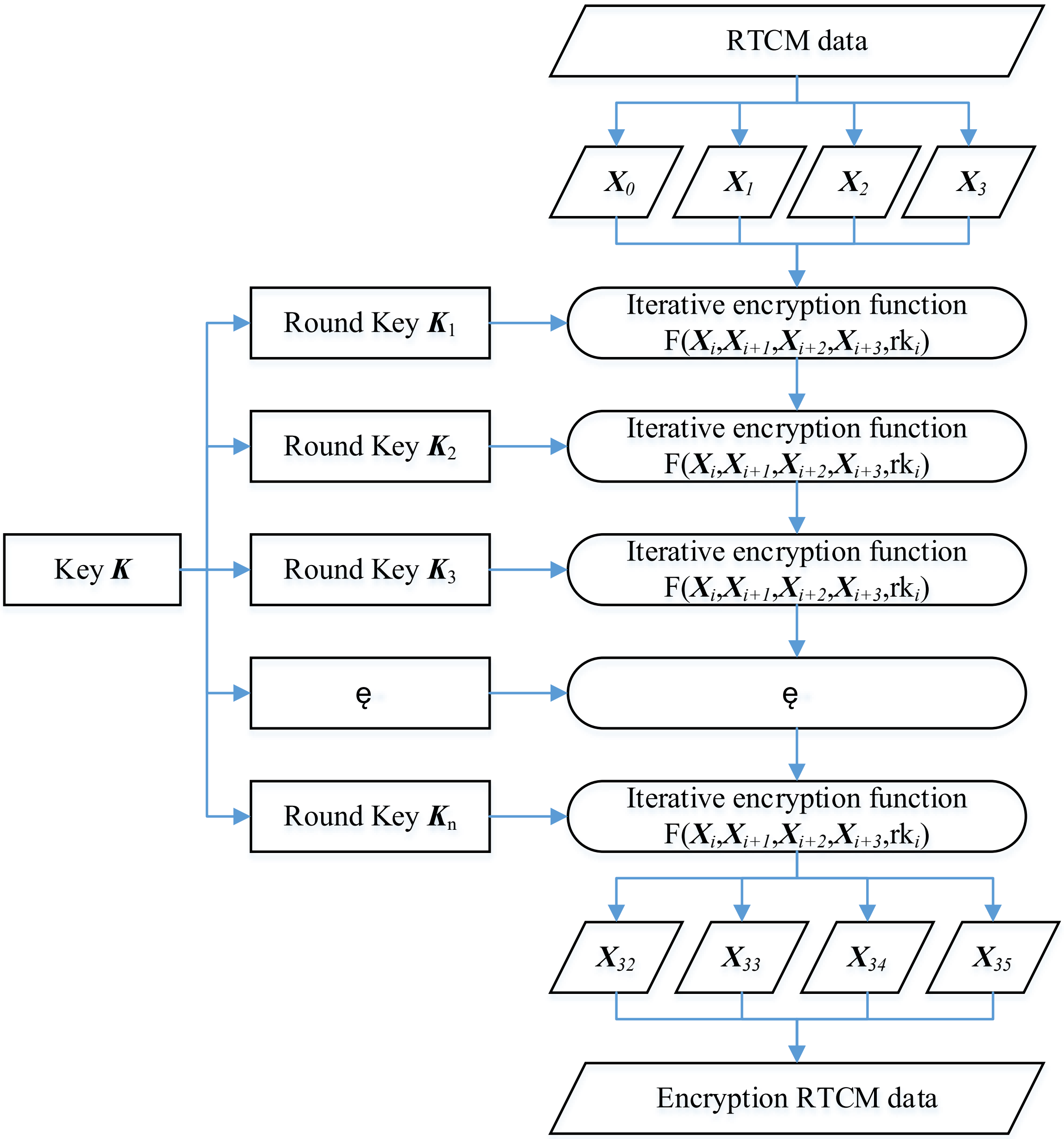
RTCM data
X_0
X_1
X_2
X_3
Key K
Round Key K_1
Round Key K_2
Round Key K_3
ę
Round Key K_n
Iterative encryption function F(X_i,X_{i+1},X_{i+2},X_{i+3},rk$_i$)
Iterative encryption function F(X_i,X_{i+1},X_{i+2},X_{i+3},rk$_i$)
Iterative encryption function F(X_i,X_{i+1},X_{i+2},X_{i+3},rk$_i$)
ę
Iterative encryption function F(X_i,X_{i+1},X_{i+2},X_{i+3},rk$_i$)
X_{32}
X_{33}
X_{34}
X_{35}
Encryption RTCM data

Figure 3. Iterative encryption of RTCM data.

GNSS RTCM data are to be encrypted. They are divided into four blocks consisting of 128 bits for each block, denoted as (X_0, X_1, X_2, X_3). Suppose (Y_0, Y_1, Y_2, Y_3) are the output encryption RTCM data; the encryption method is as follows:

$$(Y_0, Y_1, Y_2, Y_3) = R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32})$$

where R is an inverse transformation function. $X_{\boldsymbol{i}}$ can be expressed as follows:

$$X_{\boldsymbol{i}\,+\,\mathbf{4}} \mathbf{=} X_{\boldsymbol{i}} \oplus T'(X_{i\,+\,1} \oplus X_{i\,+\,2} \oplus X_{i\,+\,3} \oplus rk_i) \qquad i = 0, 1, 2, \ldots, 31,$$

where rki is the round key generated by encryption cipher, which can be expressed as the following:

$$rk_i = K_{i\,+\,4} = K_i \oplus T(K_{i\,+\,1} \oplus K_{i\,+\,2} \oplus K_{i\,+\,3} \oplus CK_i)$$

where CK_i is 32 constants of 32 bits; K_i is determined by the xor operation between the cipher and constant, both of 128 bits; and T and T' can be found in [25].

Truly random numbers generated by the cryptographic module improve the security of the encryption key, but it is not safe if the truly random number is open to the internet. To protect the truly random number, an SM2 algorithm is used. SM2 is an elliptic curve public key cryptography algorithm that uses different keys for data sending and receiving to encrypt and decrypt the encryption RTCM data. The GNSS data center generates a pair of public and private keys, in which the public key is sent to the GNSS station receiver or other data-collecting device for encrypting the data and the private key stored in the GNSS data center for decrypting the data. Compared to SM4, SM2 is a more complicated algorithm with lower encryption and decryption velocities and higher security.

According to the SM2 encryption algorithm, some public parameters are agreed to by both the data center and receiver. These parameters include a prime number p, an elliptic curve defined on finite field E, and an nth basic point on the elliptic curve G. If (x_1, y_1) and (x_2, y_2) are two points on the elliptic curve, and k is a truly random number ($k \in [1, n-1]$), a new point C_1 and a public key P can be obtained by the following:

$$C_1 = kG = (x_1, y_1)$$

$$kP = (x_2, y_2)$$

Then, the encryption key C is obtained by joining three parameters, given a random key M and the length $mlen$:

$$C = C_1 \| C_2 \| C_3$$

where $C_2 = M \oplus KDF(x_2 \| y_2, mlen)$ and $C_3 = H(x_2 \| M \| y_2)$; $KDF(x_2 \| y_2, mlen)$ is a key derivation function; and H is a compliant hash function.

5. Multiple Cryptographic Algorithms for GNSS Encryption and Decryption

A GNSS receiver can be used in a GNSS reference station, a low-cost GNSS monitoring station, and an intelligent terminal. It is different among these applications because of the diversity of hardware and operation systems. Therefore, a customized encryption plan is necessary for these hardware and operation systems. For example, the SSL protocol based on a Virtual Private Network (SSL VPN) can be used for the Linux operation system in a GNSS reference station, while it is not adaptive for an ARM operation system in a low-cost GNSS monitoring station; however, it can be developed with that requirement. We tried to give a general encryption plan for GNSS RTCM data transmission (Figure 4), which could be changed with the needs of practical conditions. The encryption method of GNSS data transmission was expressed as Algorithm 1.

Algorithm 1: Encryption steps of GNSS data transmission

```
**Input:** GNSS data, a digital certificate from a GNSS data center
**Output:** the encrypted GNSS RTCM data, the encryption key, the digest value, and the signed inspection certificate
**if** identical authentication pass **then**
An SSL VPN to be established between GNSS stations and the GNSS data center
    **if** SSL VPN established **then**
        a. generating a truly random number by cryptographic module embedded in the GNSS development board as an encryption key
        b. encrypting the GNSS data with the encryption key of an SM4 algorithm by cryptographic module
        c. extracting the public key from a digital certificate
        d. encrypting the encryption key with the public key
        e. calculating the digest value of GNSS encryption data with an SM3 algorithm by the cryptographic module
        f. signing the digest value with an SM2 algorithm by the cryptographic module to obtain a signed inspection certification and identify the certification of GNSS stations
        g. outputting all data including the encrypted GNSS RTCM data, the encryption key, the digest value, and the signed inspection certification
        h. transmitting all data to the GNSS data center by the communication module embedded in the development board.
    **end if**
**end if**
```

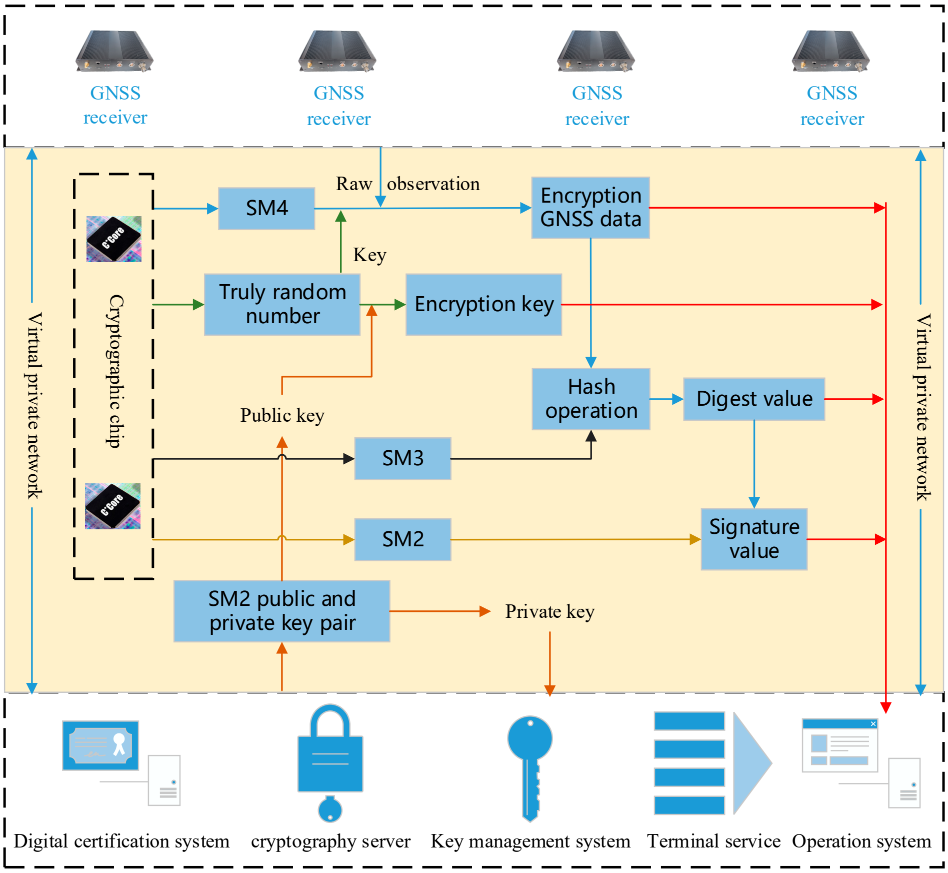

Figure 4. The flow chart of GNSS RTCM data encryption.

When the encryption GNSS RTCM data are received in the GNSS data center, the signed inspection certificate is firstly identified to adjust the credibility of the data transmission status. If it is not credible, the data are rejected because they may be unsafe. Otherwise, the encryption data key is decrypted to obtain the private key through the index of the SM2 private key. After that, GNSS RTCM data can be obtained using the SM4 algorithm to encrypt GNSS RTCM data. Finally, the digest value of GNSS RTCM data is calculated by the SM3 algorithm to compare with the transmitted digest value for the integrity test.

In the field of the GNSS real-time differential service, the method is similar to the GNSS data transmission plan. There are SSL VPN, SM2, SM3, and SM4 algorithms for encryption, decryption, and integrity protection. Compared to GNSS stations transmitting data to the GNSS data center, the difference is that the GNSS data center encrypts the real-time differential correction data and broadcasts to users through the SSL VPN. The users receive the encrypted real-time differential correction data and decrypt them for navigation and positioning.

6. Experimental Analysis

Cryptographic algorithms were firstly implemented in GNSS navigation and positioning. The process was mainly related to two parts: a GNSS station and a GNSS data center. To validate the feasibility of GNSS data encryption transmitting, we developed a GNSS receiver integrated with a cryptographic module (Section 6.1) and performed a real test in an open environment (Section 6.2). When the receiver collected different numbers of satellites, the GNSS data were not the same. At the same time, a GNSS center could receive the data from several stations to thousands of stations. Therefore, we tested the performance of a GNSS data center under the conditions of different sizes of GNSS data and different numbers of GNSS stations (Section 6.3).

6.1. Development of a GNSS Receiver Integrated with a Cryptographic Module

To test the multiple cryptographic algorithms for GNSS encryption and decryption, we developed a GNSS sensor with a GNSS development board, cryptographic module, and a 4G communication module (Figure 5). The GNSS development board was able to track multiple types of GNSS signals such as BDS B1I/B2I, GPS L1/L2, GLONASS L1/L2, Galieo E1/E5b, and QZSS L1/L2. It had 432 channels and supported global signals of BDS3. The cryptographic chip was CCM3310S-T, which supported multiple commercial cipher algorithms, such as SM2, SM3, and SM4. The highest system frequency of the cryptographic chip using 32 bits of RISC CPU reached up to 60 MHz. The 4G communication module was SLM730 C7B for all kinds of networks and multiple network systems such as TDD-LTE, WCDMA, CDMA, and GSM.

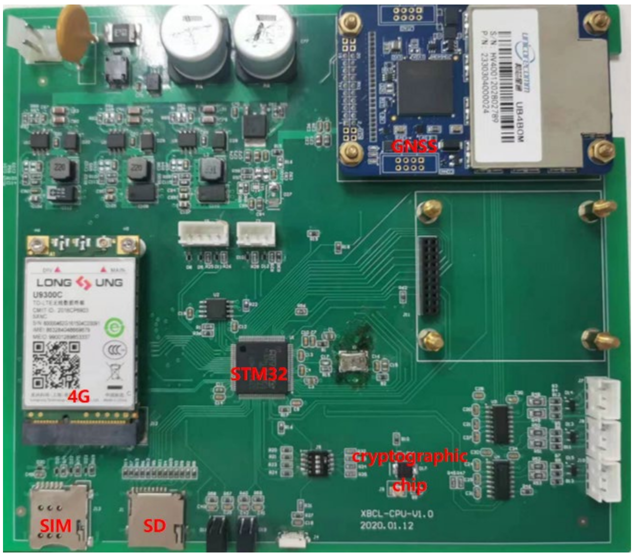

Figure 5. GNSS development board integrated with cryptographic module.

The experiment was designed to test our GNSS data encryption method using an RTK mode. We used a GNSS receiver as a reference station, and another GNSS receiver as a rover station. The encryption data of both the reference station and rover station were transmitted to a GNSS data server through a 4G network. The condition was suitable for RTK and network RTK applications.

6.2. Validation of Data Encryption in GNSS Receiver

The GNSS sensor integrated with cryptographic technology above was firstly developed to protect the data and service security. The GNSS sensor encrypted GNSS RTCM data, and the GNSS data center received and decrypted the data successfully, which ensured that the technical plan was feasible. At the same time, we needed to assess the performance of the upgraded GNSS sensor to confirm that they satisfied the time delay requirements in various applications. Therefore, the encryption time delay of GNSS RTCM data in the GNSS sensor and the decryption time delay of RTCM data and encryption time delay of real-time differential correction in the GNSS data center were operated.

To identify if the data transmission and reception of the GNSS sensor after being integrated with the cryptographic module available, we set up a reference station and a rover station with the developed GNSS board to encrypt GNSS RTCM data in an open environment (Figure 6). Two stations observed GNSS satellites simultaneously. The time of the GNSS sensor receiving GNSS satellite signals was denoted as t_1, and t_2 was the time of GNSS satellite signals between the data being encrypted by the cryptographic module and transmitted to the GNSS data center by the 4G communication module. Then, the encryption time delay of the GNSS RTCM data in the GNSS sensor was expressed as follows:

$$t = t_2 - t_1$$

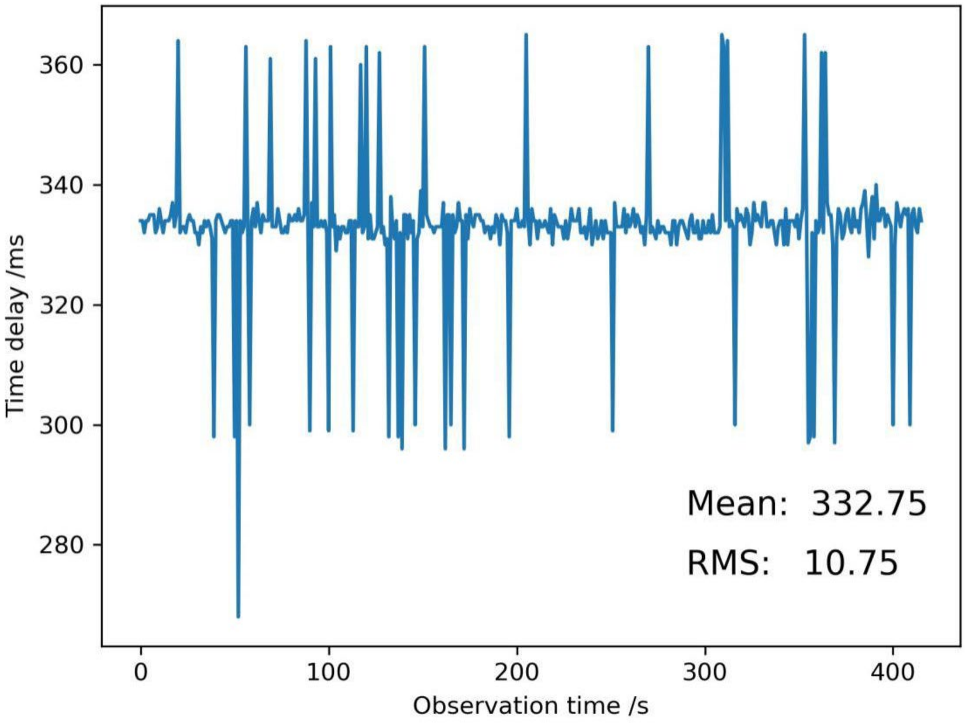

Figure 6. Encryption time delay of GNSS RTCM data in a GNSS sensor.

A series of encryption time delays of GNSS RTCM data were recorded (Figure 6). The mean encryption time delay value was 332.75 ms, and this was not a small time delay for GNSS applications. The reason for this was perhaps that the performance of the cryptographic module was to be improved, or the peripheral component interface express (PCIE) used in the paper was to be changed. The root mean square value (RMS) was 10.75 ms, which can be acceptable.

Encryption GNSS RTCM data were transmitted from a GNSS receiver to a GNSS data center through a 4G network. Every epoch's data were different because of the different satellite systems and satellite numbers. A CAT4 communication module could transmit up to 750 bytes each frame, with a 50 mbps uplink data transmission rate. When encryption GNSS RTCM data were more than 750 bytes, the GNSS RTCM data were divided into two or more frames for transmission. After commercial cryptography updating, the average transmission time was increased by 2%, which could be ignored in GNSS applications.

6.3. Simulation Encryption and Decryption Concurrent Validation of a GNSS Data Center

When the GNSS data center received the GNSS RTCM data from a GNSS station, the GNSS data center decrypted the encryption GNSS RTCM data for various applications and encrypted them again for storage by calling a cryptography server. Therefore, if there were huge GNSS stations, the performance of the GNSS data center was of crucial importance to support real-time service.

Generally, processing GNSS stations are not the same for various services. If a GNSS is used for deformation monitoring, bridge monitoring, and dam monitoring, there would be 3~10 GNSS stations. When a GNSS is used for a provincial real-time differential correction service, there would be 50~100 GNSS stations, which is dependent on the province area and topographical environment. As we know, GNSS PPP is a positioning mode, with the needs of precise satellite orbit and satellite clock products, which are generated by 100~150 GNSS stations. The other mode is network RTK, whose real-time differential corrections come from thousands of GNSS stations. The number of GNSS stations was selected from 5 to 150 to test the encryption performance, with 1000 GNSS stations as the maximum number due to limitations of the testing software.

At the same time, the size of transmitted GNSS RTCM data varied according to environmental conditions of the GNSS sensor. The size was perhaps less than 750 bits because of several visible satellites in the urban- and forest-sheltered environment, and more than 2048 bits in an open environment due to more satellites being available. Therefore, we simulated different sizes of GNSS RTCM data, from 704 bits to 5120 bits, which could cover the entire range of data.

A cryptography server from Westone Information Industry Inc. was selected to test the performance and stability. The recorded time was the difference between starting to decrypt the encryption GNSS RTCM data by calling the cryptography server and returning the plaintexts to the GNSS data center. The simulated results are shown in Figure 7. When the number of GNSS stations was five, the mean time delay was the largest among all simulated numbers of stations, and the optimal performance of the cryptography server was when the station number was equal to 40~50 stations. The performance of the cryptography server decreased with an increase in the station numbers when the station number was larger than 50. As a result, multiple cryptography servers were configured as a cluster if the station number was more than 50. Meanwhile, the performance was almost the same if the size of the data was 704 bits to 1024 bits. When the size was larger than 1024 bits, the mean time delay increased significantly at the optimal station numbers. When the number was between 60 and 150, the performance of 2048 bits was also the same as less than 2048 bits. The mean time delay increased with the growing size of the data, among all station numbers.

The mean time delay could describe the whole encryption performance of the cryptography server. To evaluate the stability of the cryptography server, the time delay difference between the maximum and the minimum of the time delay series was determined (Figure 8). The maximum time delay difference was less than 0.008 ms, which would satisfy the requirements of GNSS applications.

The data rates of the cryptography server were fixed. We estimated an index of the million bits per second (mbps) to validate the optimal configuration of station numbers and data volumes (Figure 9). If the size of the data was more than 2048 bits, a cryptography server could support 20 simultaneous encryption and decryption stations; otherwise, the number of the stations was 50. A cluster of cryptography servers should be configured if the station number exceeds the numbers.

The decryption performance of the same cryptography server was also tested according to different simulated stations and data volumes (Figure 10), which were the same as the encryption performance. When the station number was larger than 60, the decryption performance had little relationship with the data volumes; however, it was also not good if the stations were too few.

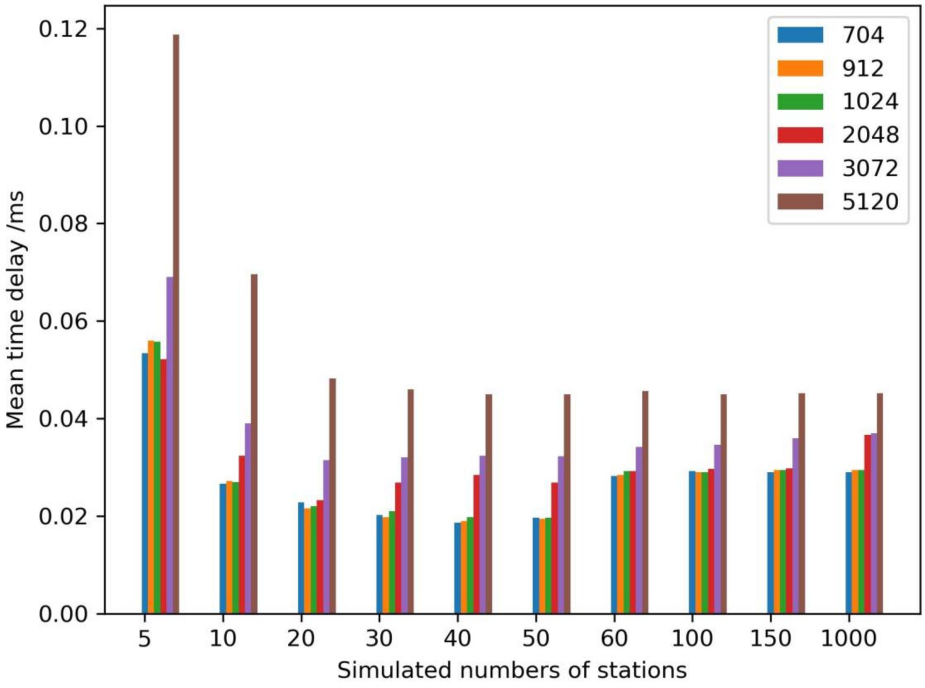

Figure 7. Encryption time delays of different simulated data volumes/bit.

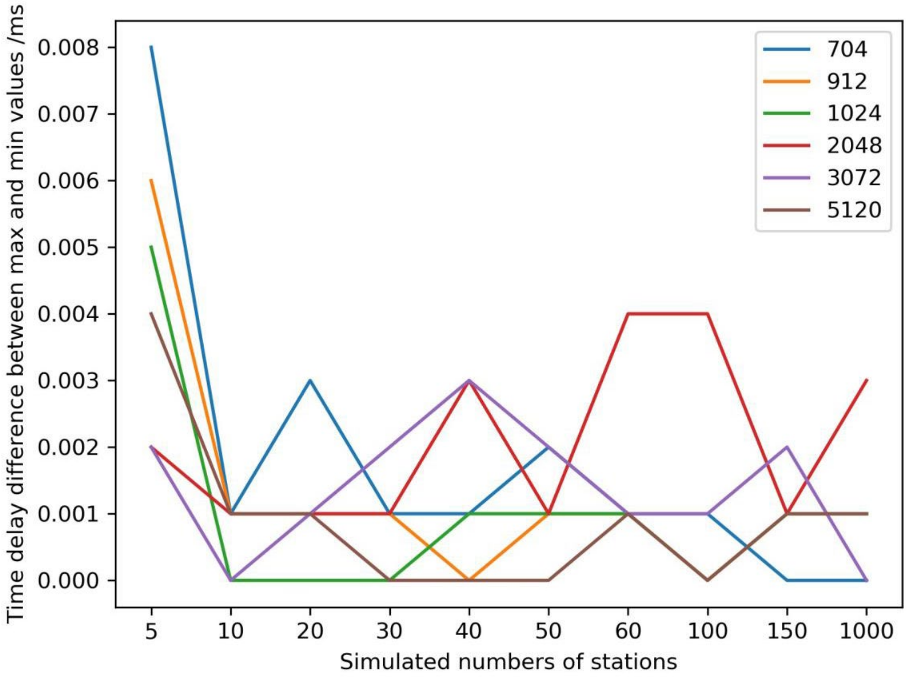

Figure 8. Encryption time delays of different simulated data volumes/bit.

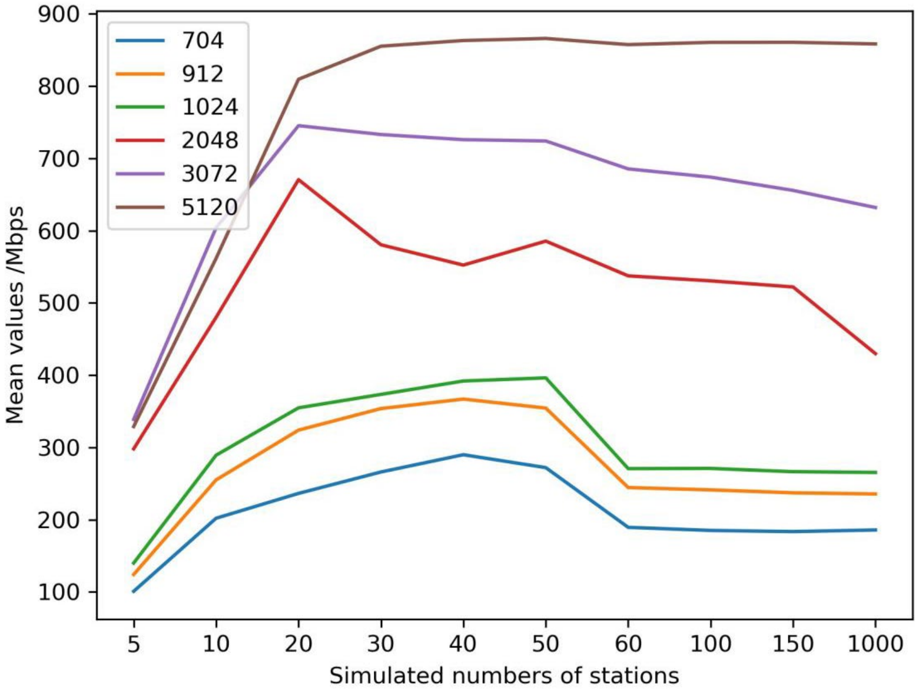

Figure 9. Encryption global rates of different simulated data volumes/bit.

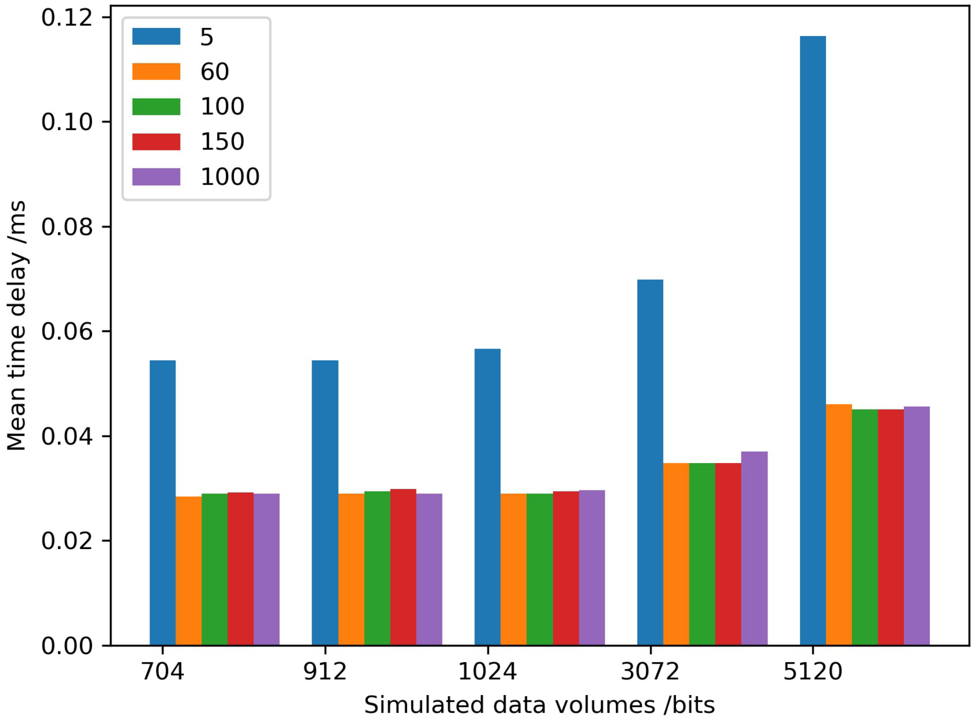

Figure 10. Decryption time delays of different simulated data volumes/bit.

7. Conclusions

From the perspective of solving the contradiction between the development and security of GNSS navigation and positioning, this study designed an upgraded structure of GNSS data transmission and service using cryptographic technology to improve the security of GNSS RTCM data from a GNSS station to a GNSS data center, and of real-time differential corrections from a GNSS data center to an intelligent terminal. This research proposes a multiple cryptographic fusion algorithm to achieve the confidentiality protection of GNSS data and service.

The developed GNSS sensor with the cryptographic module in this study has a mean encryption time delay of 332.75 ms, which is a little long for GNSS applications to be improved further, hence cryptographic software is suggested for GNSS sensor integration now. At the same time, the time delay on internet transmission caused by added encryption data can be ignored. For a GNSS data center, the time cost is less than 0.04 ms when the data volumes are smaller than 5120 bits, and the stability of the cryptography server is about 0.008 ms. Therefore, the performance of the cryptography server is satisfactory for the encryption and decryption requirements of GNSS applications. However, a cryptography server is not suitable for many stations, such as for more than 60 stations. When a GNSS data center collects from more than 60 stations, this study suggests a cluster of cryptography servers to be configured according to each cryptography server with 40~50 stations.

The proposed technical structure and upgrading method are suitable not only for traditional reference data transmission and real-time differential correction service but also for low-cost GNSS applications with an ARM platform that are used for various monitoring receivers and high-precision location services, such as intelligent terminals, wearable devices, and special vehicles. Furthermore, other controlled data collections and services are also able to use the proposed structure to improve security, such as ocean data collection and transmission, and transportation data monitoring.

Author Contributions: Conceptualization, C.X.; methodology, C.X., J.Z. and Z.Z.; software, C.X., J.Z. and Z.Z.; validation, C.X., J.Z., J.H. and X.W.; formal analysis, C.X., J.Z., J.H. and X.W.; investigation, C.X., J.Z. and Z.Z.; writing—original draft preparation, C.X. and J.Z.; writing—review and editing, C.X., Z.Z. and J.H.; visualization, J.Z. and X.W.; funding acquisition, C.X., J.Z. and Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Key Research and Development Program of China (Grant No. 2020YFB0505802), the Open Fund of State Key Laboratory of Satellite Navigation System and Equipment Technology (Grant No. CEPNT-2021KF-14), the Fundamental Research Funds of Chinese Academy of Surveying & Mapping (Grant No. AR2214) and supported by the Innovation Studio of Zhang Zhiyou.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: At the point of finishing this paper, I would like to express my sincere thanks to all those who have helped in the course of writing this paper. First of all, I would like to take this opportunity to show my sincere gratitude to Pan, who has given me some advice on the encryption of GNSS stations. Second, I would like to express my gratitude to those leaders and working staff, especially those in the institute of Geodesy and Geodynamics. Without their help, it would be much harder for me to finish my experiment in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Du, Y. Research on Algorithm and Application of High-Continuity GNSS Real-time Landslide Monitoring. Ph.D. Thesis, Chang'an University, Xi'an, China, 2022. [CrossRef]
2. Huang, G.; Wang, D.; Du, Y.; Zhang, Q.; Bai, Z.; Wang, C. Deformation Feature Extraction for GNSS Landslide Monitoring Series Based on Robust Adaptive Sliding-Window Algorithm. *Front. Earth Sci.* **2022**, *10*, 884500. [CrossRef]
3. Xi, R.; He, Q.; Meng, X. Bridge monitoring using multi-GNSS observations with high cutoff elevations: A case study. *Measurement* **2021**, *168*, 108303. [CrossRef]
4. Zhang, Q.; Ma, C.; Meng, X. Galileo Augmenting GPS Single-Frequency Single-Epoch Precise Positioning with Baseline Constrain for Bridge Dynamic Monitoring. *Remote Sens.* **2019**, *11*, 438. [CrossRef]
5. Yang, S.; Xu, C.; Mi, J.; Gu, S. Dynamic Deformation Monitoring of Offshore Oil Platforms with Integrated GNSS and Accelerometer. *Sustainability* **2022**, *14*, 10521. [CrossRef]

6. Liu, X.; Wang, J.; Li, W. A Time-Frequency Extraction Model of Structural Vibration Combining VMD and HHT. *Geomat. Inf. Sci. Wuhan Univ.* **2021**, *46*, 1686–1692. [CrossRef]
7. Li, W.; Hancock, C.; Yang, Y.; Wang, J.; Meng, X. Dynamic deformation monitoring of an offshore platform structure with accelerometers. *J. Civil Struct. Health Monit.* **2022**, *12*, 275–287. [CrossRef]
8. Zhou, F.; Dong, D.; Li, W.; Jiang, X.; Wickert, J.; Schuh, H. GAMP: An open-source software of multi-GNSS precise point positioning using undifferenced and uncombined observations. *GPS Solut.* **2018**, *22*, 33. [CrossRef]
9. Yuan, Y.; Hou, P.; Zhang, B. GNSS undifferenced and uncombined data processing and PPP-RTK high-precision positioning. *Acta Geod. Cartogr. Sin.* **2022**, *51*, 1225–1238. [CrossRef]
10. Liu, Z.; Li, Z.; Wang, C.; Yang, Z.; Yang, X. Assessment of GPS/BDS Precise Point Positioning Performance with BDS-3 New Signals. In *China Satellite Navigation Conference (CSNC 2021) Proceedings*; Yang, C., Xie, J., Eds.; Lecture Notes in Electrical Engineering; Springer: Singapore, 2021; Volume 772. [CrossRef]
11. Chen, M.; Wu, J.; Xu, C.; Bu, X. Research on grid high precision satellite navigation and positioning service method. *Sci. Surv. Mapp.* **2020**, *45*, 53–58. [CrossRef]
12. Li, X.; Zhang, X.; Ge, M. Regional reference network augmented precise point positioning for instantaneous ambiguity resolution. *J. Geod.* **2011**, *85*, 151–158. [CrossRef]
13. Geng, J.; Shi, C.; Ge, M.; Dodson, A.H.; Lou, Y.; Zhao, Q.; Liu, J. Improving the estimation of fractional-cycle biases for ambiguity resolution in precise point positioning. *J. Geod.* **2012**, *86*, 579–589. [CrossRef]
14. Ge, M.; Gendt, G.; Rothacher, M.; Shi, C.; Liu, J. Resolution of GPS carrier-phase ambiguities in Precise Point Positioning (PPP) with daily observations. *J. Geod.* **2005**, *82*, 389–399. [CrossRef]
15. Zhang, X.; Hu, J.; Ren, X. New progress of PPP/PPP-RTK and positioning performance comparison of BDS/GNSS PPP. *Acta Geod. Cartogr. Sin.* **2020**, *49*, 1084–1100. [CrossRef]
16. Yang, H.; Cheng, P.; Xu, Y.; Liu, Y.; Leng, H. BDS/GPS undifferenced RTK positioning software implementation and performance analysis using smartphone. *Sci. Surv. Mapp.* **2022**, *47*, 8–15. [CrossRef]
17. Zeng, S.; Kuang, C.; Li, Y. Data accuracy and stochastic characteristic of navigation satellites in smartphones. *J. Navig. Position.* **2020**, *8*, 88–95. [CrossRef]
18. Zhang, K.; Papadimitratos, P. Secure Multi-constellation GNSS Receivers with Clustering-based Solution Separation Algorithm. In Proceedings of the 2019 IEEE Aerospace Conference, Big Sky, MT, USA, 2–9 March 2019; pp. 1–9. [CrossRef]
19. Zhang, K.; Spanghero, M.; Papadimitratos, P. Protecting GNSS-based Services using Time Offset Validation. In Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, OR, USA, 20–23 April 2020; pp. 575–583. [CrossRef]
20. Papadimitratos, P.; Jovanovic, A. GNSS-based positioning: Attacks and Countermeasures. In Proceedings of the 2008 IEEE Military Communications Conference (MILCOM 2008), San Diego, CA, USA, 16–19 November 2008; pp. 1–7. [CrossRef]
21. Zhang, K.; Papadimitratos, P. On the Effects of Distance-decreasing Attacks on Cryptographically Protected GNSS Signals. In Proceedings of the 2019 International Technical Meeting of The Institute of Navigation (ION ITM 2019), Reston, VA, USA, 28–31 January 2019; pp. 363–372. [CrossRef]
22. Wesson, K.; Rothlisberger, M.; Humphreys, T. Practical cryptographic civil GPS signal authentication. *Navigation* **2012**, *59*, 177–193. [CrossRef]
23. Humphreys, T. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1073–1090. [CrossRef]
24. Caparra, G.; Sturaro, S.; Laurenti, N.; Wullems, C.; Ioannides, R.T. A Novel Navigation Message Authentication Scheme for GNSS Open Service. In Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), Portland, OR, USA, 12–16 September 2016. [CrossRef]
25. Huo, W.; Guo, Q.; Ma, Y. *Commercial Cryptography Application and Security Evaluation*; Publishing House of Electronics Industry: Beijing, China, 2021.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.