Design of Satellite Ranging System Based on Physical Random Sequence

Qingding He[1, a], Yongming Nie[1, b *], Huifeng Liu[1, c] and Xin Ding[1, d]

[1]China Satellite Maritime Tracking and Controlling Department, Jiangsu, Jiangyin, China, 214431

[a]nwy1986@163.com, [b]nwy1986@163.com, [c]290505026@163.com, [d]yimonie@163.com

*The corresponding author

Keywords: Telemetry tracking and controlling; Ranging system; Physical random sequence; Time synchronization

Abstract. A setup of satellite ranging based on phsical random sequence is demonstrated, which has absolute security in information transmission because of the random property of the physical sequence. Using true random sequence replacing pesudo random sequence, synchronization technology is vital important for transmitted information demodulation, despreading and decryption. Based on the pricinple of telemetry tracking and controlling system and unique properties of the phsical random sequence generating device named weakly coupled $GaAs/Ga_{0.55}Al_{0.45}As$ superlattices, a combined synchronization control system is designed, which combined the out reference clock synchronization with the chaotic synchronization. Moreover, a ranging system based on noncoherent physical random sequence spread spectrum method is investigated in detail, which is an important part of the satellite tracking and controlling system.

Introduction

An all-electronic physical random number generator that can generate random number up to 80 Gbit/s at room temperature was demonstrated in recent years, which has important potential applications in information security of satellite telemetry tracking and controlling (TT&C) area [1]. In reality, most random numbers used in computer programs are pseudo-random, which means they are generated in a predictable fashion using a mathematical formula [2-6]. This is fine for many purposes and is enough to use in many area, but it may not be random enough in normal information secure [7-10]. Ranging system is an important part of the satellite tracking and controlling system that is an information channel between the satellite and ground station opening a window to ensure the satellite being in accordance with the expected orbit and attitude. At present, generally radio wave is used for ranging in TT&C. There are four major type methods named pulse radar ranging, pure side tone ranging, pseudo code ranging and sound code mixed ranging, which are very mature. However, if true random sequence replaced pesudo random sequence for spreading and encryption, the system referring time synchroniztion should be redesigned no matter coherent or noncoherent random sequence ranging methods being used. In this manuscript, the theories of random sequence encrypttion and ranging are firstly investigated. Then, information exchange between satellite and ground station model is designed. At last, a combined synchronization control system is designed, which combined the out reference clock synchronization with the chaotic synchronization.

Theory Analyses

Encryption target is to decrease the relation between the plaintext and the ciphertext through nonlinear operations and a random number sequences, which can be designed by using chaotic systems or based on fractal shapes [11-13]. Symmetric encryption algorithms can be classified into stream ciphers and block ciphers where the image-pixels are encrypted one-by-one in stream ciphers and using blocks of bits in block ciphers. Although block ciphers require more hardware and memory, their performance is generally superior to stream ciphers since they have a permutation phase as well

as a substitution phase. As suggested by Shannon, plaintext should be processed by two main substitution and permutation phases to accomplish the confusion and diffusion properties [14]. Here we just give the basical theory analysis for its simplicity. Processes of encryption and decription of both ground station and satellite shown in Fig. 1 have the same caculting method.

At the ground station, the physical random binary bit number can be as following.

$$X(i) = x(1) + x(2) + x(3) + \cdots + x(i) \tag{1}$$

The information that should be transmitted to satellites can be written as the following expression.

$$Y(j) = y(1) + y(2) + y(3) + \cdots + y(j) \tag{2}$$

If parameter i equals to j, at the ground station, the information can be encryted based on the simple key stream encryption method, which has the form as follows.

$$S_{up} = X \oplus Y \tag{3}$$

S_{up} is the encrypted information up to the satellites, which has the same random characteristic with the physical random binary bit number X according to the properties of exclusive or operation.

On the satellite, the key number is actual the physical random binary bit number X. But there is a time delay τ. So the information after data processing by the satellite can be written as follows.

$$S = X_{\tau} \oplus (X \oplus Y) \tag{4}$$

If τ is zero, it is easy to obtain the information based on formula (4).

$$S = Y \tag{5}$$

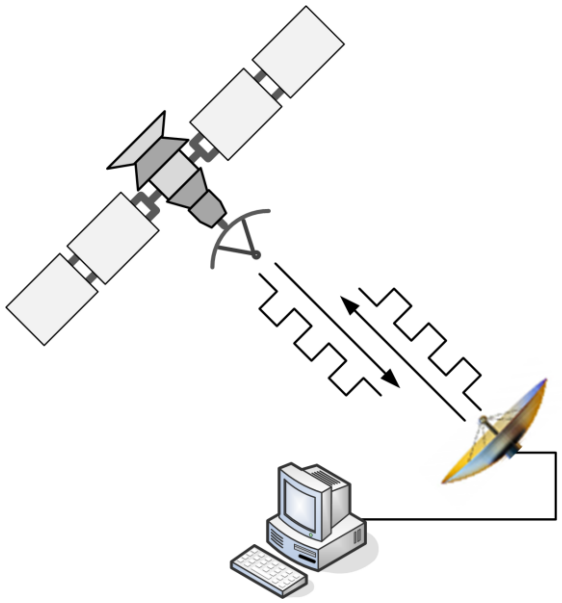

Figure 1. Schematic of information transfer between ground station and satellites

By the analysis above, it is not difficult to find that the key process of obtaining information is the delay controlling, which will be detailed analyzed later.

The radio ranging technology is based the theory basic that radio wave travels in straight line at a constant speed in space. Satellite ground station transmits a particular ranging signal, which is turning around or regenerated by satellite back to the ground station. As long as the time T is abtained, the satellite distance can be caculated according to the radio wave propagation velocity that is generally marked as c.

$$R = C \times T / 2 \tag{6}$$

It should be indicated that the time T not only includes the time light passing through the space but also the delays including ground station device signal processing time delay and satellite device signal processing time delay.

System Designations

The initial signal of semiconductor weakly coupled superlattices is only analog signal, which should be furtherly dealt with by analog-digital converting and differencing to obtain a binary physical bitstream numbers. The syetem needs two semeconductors to generate random sequence used as encrytion keys as shown in Fig. 2.

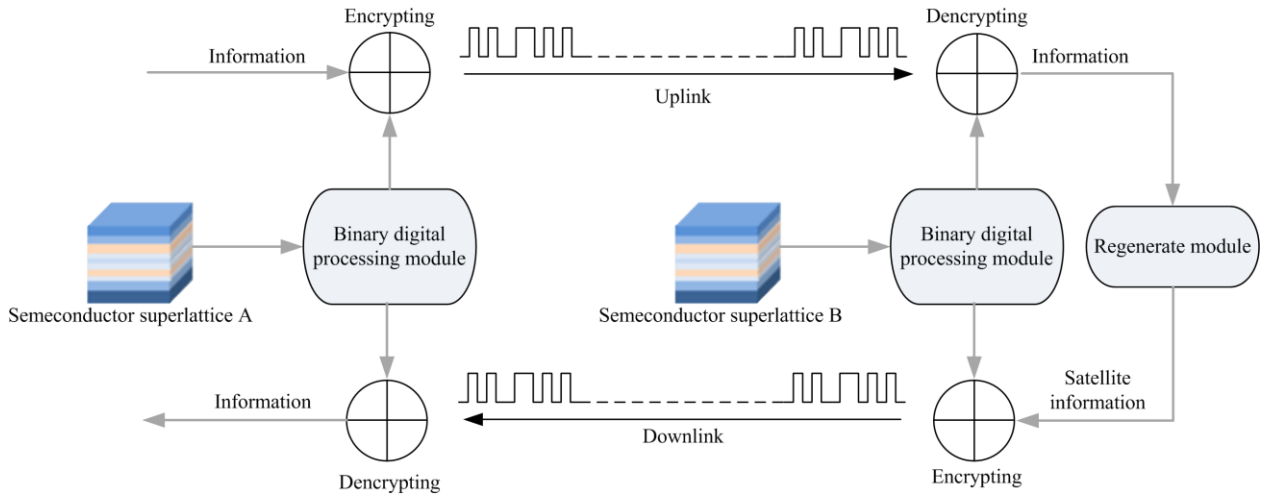

Figure 2. Schematic of information exchange between satellite and ground station

Ciphertext is obtained by encryption the plaintext with random sequence generated by semeconductor superlattice after binary digital processing. Then, the ciphertext is tansmitted to the satellite through uplink channel after up-conversion. On the satellite the received chiphertext is dencrypted by the random sequence generated by semeconductor superlattice. The plaintext is obtained on the satellite. Then the processor on the satellite regenerates another ciphertext that is similar to the process on the ground, so we no longer give detailed description.

It is easy to find that the random seauence generators both on ground station and satellite should be in sychronization, which is very important for the system. The synchronisation scheme is shown is Fig. 3

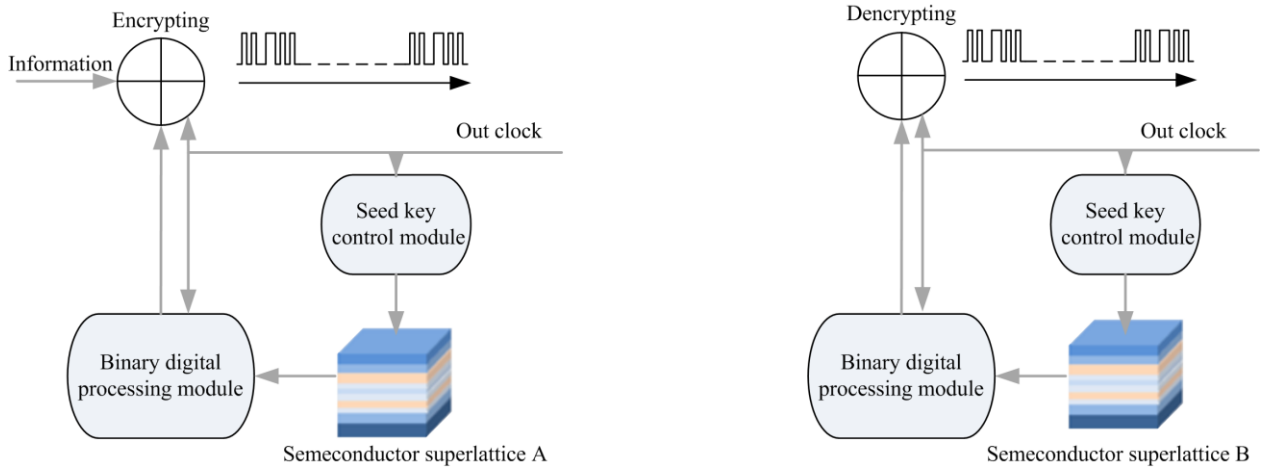

Figure 3. Schematic of time synchronization system

The left part shows the ground station sub system and the right part shows the satellite sub system. During each part, the synchronization including semeconductor superlattice, encrytion module, binary digital processing module and decryption module should be insured. Out clock can effectively afford time synchonization for each part of the system. However, there are two metods for the two semeconductors. One is the out reference clock and the other one is to use the seed key control module synchonization, which is the inherent property of the semeconductor superlattice seeing reference [1].

Conclusions

In this manuscript, a setup of satellite ranging based on phsical random sequence is demonstrated, which has absolute security in information transmission because of the random property of the physical sequence. Using true random sequence replacing pesudo random sequence, synchronization technology is vital important for transmitted information demodulation, despreading and decryption. The theories of random sequence encrypttion and ranging are firstly investigated. Then, information exchange between satellite and ground station model is designed. At last, a combined synchronization control system is designed, which combined the out reference clock synchronization with the chaotic synchronization. The designations have great significance in the information secure and ultra high speed information transmission in the future telemetry tracking and controlling system.

References

[1] W. Li, I. Reidler, Y. Aviad and et al. Fast Physical Random-Number Generation Based on Room-Temperature Chaotic Oscillations inWeakly Coupled Superlattices, Physical review letters, 111, 044102-5, 2013.

[2] M. Salvoldi and D. Choukrouny, Intersatellite Laser Ranging and Attitude Robust Measurement Planning, AIAA Guidance, Navigation, and Control Conference, 2016.

[3] G. Letchworth, X-33 Reusable Launch Vehicle Demonstrator, Spaceport and Range, AIAA SPACE Conference & Exposition, 2011.

[4] R.C.D. Raxter, Design of an S-band Transponder Providing Command, Telemetry, Ranging, and Range Rate Functions for Scientific Satellites, AIAA/CASI 6th communications satellite system conference, 1976.

[5] J. Tang， S. Xie and W. Wang, Pseudo Code Ranging Method and Precision Analysis of Aerospace Spread Spectr m TTC&DT Systems, Research and development, 4: 91-97, 2006.

[6] Q. Wu and W. Jin, Non-Coherent Ranging Technology Using Arbitrary Periodical Signal, Joumal of Astronautics, 34(3): 390-396, 2013.

[7] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical journal, 28(4): 656-715, 1948.

[8] Y. Wang, Analysis of Secure Limitation of One-Time System and Its Origin, Electronic science and technology, 21(1):71-75, 2008.

[9] W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Infromation Theory, 22(6):644-654, 1976.

[10] J. Dong, W. Zhu, X. Pu and et al, Design of a Physical True Random Number Generator, Electronics Optics＆Control, 20(2): 93-97, 2013.

[11] M. L. Barakat, A. S. Mansingka, A. G. Radwan and et al, Generalized hardware post processing technique for chaosbased pseudo random number generators, ETRI J, 35(3):448–58, 2013.

[12] M. L. Barakat, A. S. Mansingka, A. G. Radwan and et al, Hardware stream cipher with controllable chaos generator for colour image encryption, IET Image Process, 8(1):33–43, 2014.

[13] S. K. Abd-El-Hafiz, A. G. Radwan, S. H. AbdElHaleem and et al, A fractal-based image encryption system, IET Image Process , 8(12):742–52, 2014.

[14] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int J Bifurcat Chaos, 16(8):2129–51, 2006.