A Power-Efficient and Secure Communication Scheme in Satellite Communication

Shengli Zhao\textsuperscript{1}, Xianliang Lan\textsuperscript{2} and Zihan Yu\textsuperscript{1}

\textsuperscript{1} SiChuan DMazure Information Technology Co, Ltd., Chengdu, China
\textsuperscript{2} Baotou Railway Vocational & Technical College, Baoto, China
Email: victory.zhao@dmazure.com.cn; btzylxl@hotmail.com; yu@dmazure.com.cn

Abstract. Resource is very limited in satellite communications, thus issues on security and power-efficiency in satellite communications have aroused extensive attention in recent years. In this paper, we have proposed a transmission scheme in satellite communication systems, which is secure and power-efficient. The binary bit sequence is encrypted prior to the modulation step, thus achieving security. The security analysis is based upon the Wyner wiretap model. In the wiretap model, the transmitter attempts to send messages to the legitimate receiver, meanwhile the eavesdropper is passively wiretapping. The legitimate receiver is assumed to have a good knowledge of the secret keys, so he can recover the original signal. However, the eavesdropper experiences severe interference and cannot mitigate it. The secrecy performance is measured by the secrecy rate. The secrecy rate is the rate difference between the legitimate communication and the illegal communication. Security of the proposed scheme is demonstrated by the mathematical analysis and Monte-Carlo simulations. In addition, the key space and the time needed to crack the secret keys are also calculated. The analysis results illustrate that the proposed scheme can provide a substantial security enhancement to the satellite communication system, meanwhile achieves power-efficiency.

Keywords. Satellite communication; secrecy rate; power-efficiency; wiretap model.

1. Introduction

As we know, resource is very limited in the satellite communications. Meanwhile, the transmitted information can be easily eavesdropped due to the openness nature in wireless communications. There has been a growing demand for security, spectrum and power efficiency in satellite communications. Security has also gained extensive attention in satellite communication systems recently, especially in military applications. The aim of DVB-S2 (Digital Video Broadcasting-Satellite, second generation) standard is to provide high quality broadcasting service [1]. Therefore, it is important to design a power-efficient and secure communication scheme in satellite communications.

A general structure of the wiretap model in satellite communications is depicted as figure 1, in which the legitimate transmitter intends to send messages to the legitimate receiver. The general satellite systems are inherently prone to adverse attacks, it is because the wireless communication is featured as openness. Therefore the sensitive satellite information can be easily intercepted and illegally utilized. The eavesdropper can make full use of the intercepted information, thus some sensitive information can be leaked.

Most of the researches on the security of the satellite communication focus on the upper layers [2], which may increase implementation difficulties and vulnerabilities to adverse attacks. Most of the encryptions on the upper layers leave the address or the header information unencrypted, thus will
increase the possibilities of the information leakage. In addition, enhanced computing power of computers may crack the encrypted information, which is encrypted by the conventional encryption algorithms. The physical layer security can be a superior candidate, or at least an effective supplement to the upper layers security. Furthermore, the encryption scheme in the physical layer and the upper layer security can be combined to enhance the security of the satellite communication systems. Physical layer security has initially been proposed by Wyner [3], which aims to cause severe interferences to the eavesdropper based on the information theory. As a commonly used measure to measure the security level, The secrecy rate, which is defined as the rate difference between the legitimate link and the eavesdropping link in the Gaussian channel [4], is commonly used to measure the security level.

As to the traditional physical layer security techniques applied in satellite communications, artificial noise [5] and beamforming [6] have already been used. However, the power-efficiency is relatively low due to the additional antenna and power assumptions. The cryptographic algorithms relate to chaos have attracted much research interest recently [7], and it is widely applied in wireless communications. Chaotic sequences are featured as pseudo randomness, ergodicity and high sensitivity to initial values [8], and hence uncorrelated chaotic sequences can be generated. Confronted with the some possible severe security issues, the application of the chaos encryption is getting essential in wireless communications. As the burst of errors can be converted into seemingly random errors under the effect of chaos encryption, thereby minimizing the effect of error bursts. Moreover, the strong ability of randomization makes the information totally meaningless for the eavesdropper, thus enhancing the security level. In recent years, chaos cryptography is emerging as a novel and potential technique on the physical layer security as it can enhance both confidentiality and meanwhile achieve power-efficiency. In order to minimize power consumption of the satellite communication, 1 dimension logistic chaotic maps are adopted in the proposed scheme.

As the burst of errors can be converted into seemingly random errors under the effect of chaos encryption, thereby minimizing the effect of error bursts. Moreover, the strong ability of randomization makes the information totally meaningless for the eavesdropper, thus enhancing the security level. In recent years, chaos cryptography is emerging as a novel and potential technique on the physical layer security as it can enhance both confidentiality and meanwhile achieve power-efficiency. In order to minimize power consumption of the satellite communication, 1 dimension logistic chaotic maps are adopted in the proposed scheme.

![Wiretap model of the satellite communication.](image)

**Figure 1.** Wiretap model of the satellite communication.

This paper proposed a chaos-based encryption scheme in satellite communication. Thus the communication system can exhibit robustness to the adverse attacks. The bits which are processed by chaotic encryption will get utterly useless for the eavesdropper. A corresponding decryption block at the intended receiver end uses the inverse operations to recover the original information sequence, while the unintended receiver cannot extract the original signal without the right keys. Considering the low complexity of the LDPC codes, we employ LDPC codes. The encryption scheme is on the basis of the OFDM communication system and employs the chaotic encryption. It not only enhances the security level, but also enhances the power-efficiency. In the latter design, we will introduce logistic chaotic maps to the satellite communication systems. The corresponding mathematical analysis will also be performed to validate the security of the proposed scheme.
The paper is outlined as the following: In section 2, basic structure, properties of OFDM, logistic chaotic map and LDPC codes are elaborated. Section 3 presents the proposed secure transmission scheme. Corresponding mathematical analysis are performed in section 4, and Section 5 contains some concluding remarks and future work.

2. Background
In this section, we give an explanation of the basic components included in the proposed satellite communication system. Although OFDM, LDPC codes and logistic chaotic maps have already been applied in the wireless communications, their basic structure and properties are still being introduced in detail. We will elaborate the advantages of these techniques applied in the satellite communication systems.

2.1. OFDM
Faced with an increasing shortage of spectrum resource in the satellite communication, OFDM has drawn a huge amount of attention owing to its inherent properties, such as high spectral efficiency, tolerance to the frequency selective fading, simple and flexible implementation. OFDM utilizes multi-carrier modulation to achieve high reliability and high spectral efficiency [9]. Multiple mutually orthogonal subcarriers are used to transmit data in OFDM. It can improve the spectrum utilization as it decreases the influence of the frequency selective fading [10]. Thus OFDM has become the basis of many telecommunication standards. Moreover, OFDM is becoming an irreplaceable part in the communication systems such as long term evolution (LTE), 5G communications, worldwide interoperability for microwave access (WiMAX) [11].

A general OFDM digital implementation structure is described in figure 2. At the transmitter side, the series-to-parallel transformation module divides the bit sequence into a plurality of sub-signals to be transmitted and the plurality of sub-signal assigned to each subcarrier is superposed on each other. Each sub-carrier must be strictly orthogonal to each other. The modulated data is transformed into time-domain signal after IDFT. Then the sequence is transformed by the parallel-to-series and analog-to-digital process, thus composing the signal to be transmitted.

At the legitimate receiver end, inverse operations can be performed to obtain the original signal.

![Figure 2. the OFDM digital implementation structure.](image)

2.2. Logistic Chaotic Map
Many researchers have found that there is a close relationship between chaos and cryptography in recent years. The pseudorandom property of the chaotic sequence makes the bits distribute randomly, so the burst errors can be spread to a great extent. In addition, the high peak-to-average power ratio (PAPR) the general OFDM system inevitably suffers from can be reduced to a great extent with the introduce of the chaotic maps [12]. In a word, the application of the chaotic maps guarantees security and reliability simultaneously during communication.

A chaotic system is a dynamical nonlinear system. The superior security obtained by the chaotic map benefits from its non-binary nature. The chaotic mapping is a dynamic value-continuous time-discrete equation, which depicts the relationship between the current state and the next state. Its
operation does not only depend on the current symbols but also on the previous symbols. A logistic chaotic map [13] can expressed as (1).

\[ x_{n+1} = \mu x_n (1 - x_n), u \in (3.57, 4], x_n \in (0,1) \]  \hspace{1cm} (1)

In the above expression, \( \mu \) presents the bifurcation parameter, \( n \) denotes the iteration times. It has been proved that the chaotic system falls into pseudo-random chaotic state after a certain times of iteration, provided that \( \mu \) is within the range of \((3.57, 4]\) [14]. And a small discrepancy from the initial value can cause a totally different value after a certain number of iterations.

Figure 3 reveals that the system behaves differently with the increase of \( \mu \). When \( \mu \) is close to 4, the system achieve chaos. Therefore, the system behave good randomness when \( \mu \) is within the range of \((3.57, 4]\). In order to distinguish chaos or not, the Maximum Lyapunov exponent [15] is used.

2.3. Low Density Parity Check Codes

Low-Density Parity-Check (LDPC) codes, discovered by Gallager [16], show superior BER performance, which approaches the Shannon limit over the AWGN channels [17]. LDPC codes have many advantages such as low decoding complexity, low latency, therefore LDPC codes are commonly employed in the satellite communications.

LDPC codes are block codes with parity check matrices, which contain very few non-zero terms. LDPC codes have a simple graphical representation based on Tanner graph. It contains two groups of nodes, namely check nodes and variable nodes [18]. The rows and columns of the parity check matrix are represented by the check nodes and variable nodes, respectively.

Assuming that the parity-check matrix has \( M \) rows and \( N \) columns, the parity-check matrix can be expressed as a \( M \times N \) matrix. Take a \( 4 \times 6 \) parity check matrix as an example, and the tanner graph is presented as figure 4.

\[ H = \begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 \\
\end{bmatrix} \]

The commonly used decoding algorithms are Belief Propagation algorithm, Bit-flipping algorithm, and Logarithmic domain Belief Propagation algorithm [19]. The decoding complexity and the minimum distance increases with the increasing code length.

LDPC codes have many advantages such as relatively low complexity, good reliability and implementation flexibility.
3. Overview of the System Model
In this section, the systematic transmission model is presented. Figure 5 depicts the schematic diagram of the secure OFDM transmission system in the satellite communication. As viewed from figure 5, the random binary bit sequence is encoded by the LDPC coder and mapped by the logistic chaotic map. Under the effect of the logistic chaotic map, the binary bits are distributed in a totally different order, thereby completing encryption. In the practical application, the key distribution mechanism is essential, there are some referential mechanisms [20].

![System model of the proposed communication scheme.](image)

The encrypted serial sequence is converted into parallel sequence and modulated. Then the modulated signals are mapped by the chaotic maps before IDFT. Then the encrypted information sequence are processed by the IDFT module, thereby transforming into the frequency-domain signal. Finally the encrypted signals are transmitted by the antenna.

At the intended receiver end, the signals are processed by the inverse operations with the secret keys. The encryption and decryption are controlled by the secret keys. However, the unintended receiver are unable to recover the original information.

4. Performance Evaluation and Analysis
At first, we give an overview of the wiretap model, and then deduce the expression of secrecy rate, figure out the secret key space and the time needed to break the cypher. In the end, corresponding MATLAB simulations are performed to validate the feasibility and reliability of the proposed scheme.

4.1. Overview of the Wiretap Model
The wiretap model used in the following analysis is shown in figure 6, in which the legitimate Alice attempts to communicate with the legitimate receiver Bob while Eve is passively eavesdropping. All nodes are assumed to be equipped with one antenna. The signals obtained by the Bob and Eve are expressed as below.

\[ y_B = h_B s + n_B \]  \hspace{1cm} (2)

\[ y_E = h_E s + n_E \]  \hspace{1cm} (3)

In the above equation, \( s \) is the transmitted signal, \( n_B \) and \( n_E \) represent the Gaussian noise, \( h_E \) and \( h_B \) denote the channel gains of Alice-to-Eve link and Alice-to-Bob link, respectively.

The intended receiver Bob is assumed to have a good knowledge of the secret keys. Therefore Bob can recover the original signal correctly, while Eve is not capable of obtaining the original signal. In the latter analysis, the secrecy rate denotes the maximum reliable rate of information transmission in the legal links. The secrecy rate is given by (4).
Figure 6. The wiretap model.

\[ G_{sec} = \left[ C_D - C_E \right]^+ \] (4)

In the above equation \([x]^+\) denotes \([0, x]\). The capacity in the Alice-to-Bob link and the Alice-to-Eve link is denoted in (5) and (6), respectively.

\[ C_{AB} = \frac{1}{2} \log_2 (1 + \gamma_D) \] (5)

\[ C_{AE} = \frac{1}{2} \log_2 (1 + \gamma_E) \] (6)

In the above equation, \(\gamma_D\) and \(\gamma_E\) are the signal-to-noise ratio of the Alice-to-Bob link and Alice-to-Eve link, respectively. Consequently, we can get the expression of secrecy rate shown as (7).

\[ C_s = \left[ \frac{1}{2} \log_2 (1 + \gamma_D) - \frac{1}{2} \log_2 (1 + \gamma_E) \right]^+ \] (7)

4.2. Secrecy Rate Analysis

We adopt the MQAM as the modulation method in the proposed system. So within the time of \([0, T_s]\), the modulated MQAM signals on the \(i\)-th subcarrier can be denoted as equation (8).

\[ s_i(t) = A_i g(t) \cos(2\pi f_i t) - A_i g(t) \sin(2\pi f_i t) + \text{Re}\left\{A_i g(t)e^{j2\pi f_i t}\right\} = \text{Re}\left\{A_i g(t)e^{j2\pi f_i t}\right\} \] (8)

In (8), \(A_i\) denotes the transmitted QAM symbol constellation points, \(A_i\) and \(A_i\) represents the co-directional component and the orthogonal component, respectively. \(f_i = f_c + i\Delta f\) is the frequency of the \(i\)-th sub-carrier, and \(g(t)\) is the impulse response of pulse shaping filter. The OFDM signal can be expressed as (9), in which \(a(t)\) is the complex envelope of the OFDM signal in the expression of \(s(t)\).

\[ s(t) = \sum_{i=0}^{N-1} s_i(t) = \text{Re}\left\{\sum_{i=0}^{N-1} A_i g(t)e^{j2\pi f_i t} \right\} = \text{Re}\left\{a(t)e^{j2\pi f_i t}\right\} \] (9)

The complex envelope of OFDM signal is sampled to be time-discrete signal, thereby realizing the baseband digital modulation for OFDM. During the period of time \([0, T_s]\), the sampling time is set as \(m T_s/N, m = 0, 1, \ldots N-1\), and the sampled signal of the complex envelope can be denoted as (10). The below equation also describes the expression of the sequence \(\{A_i\}\) processed by IDFT.

\[ a_m = a \left( m T_s/N \right) = \sum_{i=0}^{N-1} e^{j2\pi i\Delta f m} = \sum_{i=0}^{N-1} e^{j2\pi i m/N} \] (10)
At the receiver side, the complex envelope can be recovered by the orthogonal demodulation, by which we can get the sampled time-domain sequence \( \{a_0, a_1, \ldots, a_{N-1}\} \). And after DFT, the transmitted frequency-domain sequence \( \{A_i\} \) can be denoted as (11).

\[
A_i = \sum_{m=0}^{N-1} a_m e^{-j2\pi m i / N}, i = 0, 1 \ldots N-1
\]

(11)

The sampled OFDM signal in the time domain is denoted as \( \{a_m\} \), and the signal in the frequency domain is expressed as \( \{A_i\} \). In the Alice-to-Bob link, the legitimate receiver is able to recover the signal correctly. And hence the capacity can be expressed in (12), in which \( \delta^2 \) denotes the power of Gaussian noise.

\[
C_{AB} = \frac{1}{2} \log_2 \left( 1 + \frac{\sum_{i=0}^{N-1} A_i^2}{\delta^2} \right)
\]

(12)

As to the Alice-to-Eve link, the eavesdropper is trying to break the cypher to recover the signal. We assume that there are \( \theta \) percent of bits that can be recovered correctly. Thus the capacity can be expressed as (13):

\[
C_{AE} = \frac{1}{2} \log_2 \left( 1 + \frac{\theta \sum_{i=0}^{N-1} A_i^2}{(1-\theta) \sum_{i=0}^{N-1} A_i^2 + \delta^2} \right)
\]

(13)

So we derive the expression of the secrecy rate shown as (14).

\[
C_{sec} = \left[ \frac{1}{2} \log_2 \left( 1 + \frac{\sum_{i=0}^{N-1} A_i^2}{\sigma^2} \right) - \frac{1}{2} \log_2 \left( 1 + \frac{\theta \sum_{i=0}^{N-1} A_i^2}{(1-\theta) \sum_{i=0}^{N-1} A_i^2 + \sigma^2} \right) \right]^*
\]

(14)

It is assumed that the probability of the parameter \( \theta \) obeys the normal distribution, and hence the secrecy capacity can be further expressed as (15).

\[
C_{sec} = \left[ \frac{C_{AB} - \theta \sum_{i=0}^{N-1} A_i^2}{(1-\theta) \sum_{i=0}^{N-1} A_i^2 + \sigma^2} \right]^*
\]

(15)

Based on the above equation, we obtain the curve of the secrecy rate as a function of SNR. Notice that a positive secrecy rate can be obtained in figure 7 and the proposed encryption scheme presents a superior security performance. It is worth noting that a considerable difference exists between the legal link and the illegal link.
4.3. The Secret Key Space

In our scheme, logistic maps are used to encrypt the information bits, in which initial values and bifurcation parameters serve as the secret keys. The chaotic sequence is highly sensitive to initial conditions. The experiment reveals that when the initial value or bifurcation parameter changes slightly in the order of magnitude of \(10^{-15}\), the adjacent orbits will be separated completely after more than 40 times of iterations.

The systematic parameter used in the logistic chaotic system ranges from 3.56994 to 4. So the key space of the proposed scheme is \(0.43006 \times 10^{30}\). Assuming that the computer is able to complete \(10^6\) times of computation per millisecond, the decryption time needed is \(1.365 \times 10^{13}\) years. In case the confidential information is captured by the illegal receiver, the secret keys can hardly be cracked and extracting the useful information seems impossible. Therefore, the proposed scheme can exhibit robustness to resist the exhaustive attacks.

5. Conclusion and Discussion

The proposed communication scheme has the following advantages:

In terms of confidentiality, the above mathematical analysis suggests that the proposed approach is able to provide good security enhancement of the transmission. There exists a huge secret key space and it is difficult to crack the information. Seldom can the eavesdropper break the cipher and recover the original signals correctly, and the positive secrecy rate can always be obtained.

In terms of power efficiency, the proposed scheme achieves good power efficiency. The introduced logistic chaotic maps have relatively low complexity and the implementation is relatively easy. The proposed scheme can save power and can meet the demand of the satellite communications.

With respect to flexibility, the chaotic logistic map, OFDM and LDPC code can be flexibly designed and the parameters can be set according to the practical scenario. The superior performance can be obtained at the cost of complexity, power consumed and latency. We should balance the superior performance and the cost in the practical applications.

In this paper, we propose a novel encryption method to enhance security in OFDM satellite communication systems, which exploits the pseudo random property of the logistic chaotic map. Under certain approximations, we figure out the secrecy rate the proposed system can approach. In the end, we complete the corresponding mathematical analysis to demonstrate the superiority of the proposed approach.

There still exists room for improvement in the future research. On one hand, this paper only concentrate on the logistic map used in the physical layer. Considering that the pseudo-random property of the chaotic maps can be fully utilized, we will extend the chaotic maps with the upper layers in the future, thus composing a comprehensive security system. On the other hand, we will investigate other approaches to further improve the power efficiency in the satellite communication.
References
[1] ETSI EN 302 307-1:1 2014 Digital video broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications ETSI Standard, Part 1: DVB-S2 A, (1).
[2] Bejarano J M R, Yun A and Cuesta B D L 2012 Security in IP satellite networks: COMSEC and TRANSEC integration aspects IEEE Advanced Satellite Multimedia Systems Conference pp 281-288.
[3] Wyner A D 1975 The wire-tap channel Bell Labs Technical Journal 54 (8).
[4] Leung-Yan-Cheong S, and Hellman M 1978 The Gaussian wire-tap channel IEEE Transactions on Information Theory 24 (4) 451-456.
[5] Zhou M K and McKay M R 2010 Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation IEEE Transactions on Vehicular Technology VT 59 (8) 3831-3842.
[6] Zheng G, Arapoglou P-D and Qtttersten B 2012 Physical layer security in beam-forming satellite systems IEEE Transactions on Wireless Communications 11 (2) 852-863.
[7] Liu B, Zhang L, Xin X and Wang Y 2014 Physical layer security in ofdm-pon based on dimension-transformed chaotic permutation IEEE Photonics Technology Letters 26 (2) 127-130.
[8] Zhong J, Yang X and Hu W 2017 Performance-improved secure ofdm transmission using chaotic active constellation extension IEEE Photonics Technology Letters 1-1.
[9] Gong G, Lu J, Xiong C, Duan R and Tan Z 2015 Cross-layer resource allocation based on mixed-service fairness for broadband power-line ofdm system Proceedings of the CSEE 35 (6) 1390-1398.
[10] Chen S, Chen X, Huang R, Chen Y, Lu J and Cai P 2018 Research on middle voltage power line OFDM communication strategy based on channel estimation TCSP 686-689.
[11] Islam R, Choudhury P and Islam M A 2014 Analysis of DCO-OFDM and flip-OFDM for IM/DD optical-wireless systems International Conference on Electrical and Computer (ICECE) pp 32-35.
[12] Yang X, Hajomer A, Shen Z and Hu W 2017 Security and performance improvement in OFDM transmission using chaotic precoding International Conference on Transparent Optical Networks (ICTON) pp 1-3.
[13] Liu L, Miao S, Hu H and Deng Y 2016 Pseudorandom bit generator based on nonstationary logistic maps IET Inf. Security 87-94.
[14] Bi M, Fu X, Zhou X and Zhang L 2017 A key space enhanced chaotic encryption scheme for physical layer security in OFDM-PON IEEE Photonics Journal 9 (1).
[15] Zhang J, Zhu H P, Zhu Y X and Cheng J 2016 A hybrid DS/FH signal generator based of spatiotemporal chaotic OCML IEEE ICC 2682-2686.
[16] Gallager R G 1962 Low-density Parity-check codes IRE Trans. Inf. Theory 8 (1) 21-28.
[17] Richardson T J, Shokrollahi A and Urbanke R 2001 Design of capacity approaching low-density parity-check codes IEEE Trans. Inf. Theory 47 (2) 619-627.
[18] Zhong H and Zhang T 2003 Design of VLSI implementation-oriented LDPC codes Proc. IEEE 58th Vehicular Technology Conf. pp 670-673.
[19] Costello D J and Hagenauer J 1998 Application of error correcting codes IEEE Transactions Information Theory pp 2531-2560.
[20] Taha H and Alsusa E 2017 Secret key establishment technique using channel state information driven phase randomization in multiple-input multiple-output orthogonal frequency division multiplexing IET Information Security 11 (1) 1-7.