Research and Application of Chaotic Encryption Technology in Wireless Communication

Liang Ye, Zhou Ling, Gao Nan

Lanzhou City University, Lanzhou, Gansu, 730070, China

Email: 13919372969@163.com

Keywords: chaotic encryption, wireless communication, Logistic mapping, channel equalization

Abstract: In order to improve wireless communication confidentiality and anti-interference, an optimal wireless communication technology is proposed based on the chaotic encryption technology, wireless communication channel model is firstly constructed, communication data sampling is taken, chaotic encryption of communication signal sampling is obtained, chaotic encryption algorithm uses the Logistic mapping as the basis function, the wireless communication encoding embedded in the encryption system, the Logistic maps are piecewise linear extension to complete the communication of the sequence encoding, thereby improving the plaintext, correlation between encoding and encryption, the encryption and encoding to form a unified whole, and then with the chaotic encryption, the cumulative probability interval of plaintext cyclic shift, improved random wireless communication and secrecy of chaotic sequences. The simulation results show that the encryption process using the method of wireless communication can improve the security of communication, it can effectively improve the fidelity of communication transmission, channel equalization performance is better.

1. Introduction

Wireless Electrical communication by the electromagnetic radiation interference intensity, vulnerable to attack and intrusion, and because the radio communication channel with multipath characteristics, resulting in communication transmission quality is not stable, the signal is susceptible to interference or easily intercepted, confidentiality and fidelity of information transmission is not good, in order to improve the security of wireless communication, the need for encryption design the wireless data communication[1].

Wireless communication is vulnerable to factors such as natural and channel interference, and the confidentiality of information interaction and transmission is poor, communication encryption and anti interference design is necessary to reduce the error rate of communication[2]. At present, the main method of encoding embedded encryption design of wireless communication, chaotic mapping key construction method and synchronous encoding and encryption methods, construct data encryption key encryption, combined with the source encoding of chaotic systems and secure communication, but there were some defects in the traditional encryption scheme in data security and encryption efficiency, secure communication efficiency is not good, for example, in reference [3], it proposed a kind of image encryption technology transfer DCT transform and DNA arithmetic based on the combination, and applied in wireless encryption system communication, using multi scale gradient cycle key construction and encoding design decomposition method, the communication encryption is realized, but the method in constructing the encryption key Vulnerable to known plaintext attacks, resulting in low reliability[4].

Aiming at the above problems, this paper proposes a wireless communication optimization technology based on chaotic encryption technology.

  DOI: 10.25236/icscbd.2018.027

2. Basic knowledge description and model design

2.1. Chaotic encryption basic knowledge and communication channel model

In order to improve the security of wireless communication, this paper improved chaotic encryption algorithm for wireless communication, the first to build a wireless communication channel model, wireless communication channel transmission medium is not uniform non ideal medium, radio communication channel complex, multipath structure depends on radio communication channel in radio transmission frequency and the spatial gain of wireless communication channels the transmission loss is mainly composed of extended losses and bad loss, the average transmission loss can be expressed as:

$$TL = n \cdot 10 \lg r + \alpha r \tag{1}$$

In the model, TL is radio communication propagation loss (dB), n is radio communication propagation factor, r is propagation attenuation, thus wireless communication channel model is expressed as:

$$c(\tau, t) = \sum_{n} a_n(t) e^{-j2\pi f_c \tau_n(t)} \delta(t - \tau_n(t)) \tag{2}$$

Wherein, $a_n(t)$ is the calculation of expansion of spherical wave propagation loss of linear impulse response characteristics, $\tau_n(t)$ is attenuation loss section of n path, f_c is channel intersymbol interference frequency, $s_i(t)$ is propagation attenuation coefficient. The communication channel spreads spectrum modulation method, and gets the wireless communication multipath channel impulse response:

$$h(t) = \sum_{i=1}^{P} a_i \, p(t - \tau_i) \tag{3}$$

Where, a_i and a_i are respectively corresponding to the different paths of the time and frequency resolution, after QAM modulation to obtain unipolar signal, weighting coefficient b_v', the wireless communication signal is decomposed into positive and negative signal, namely $x_k = x_k^+ + x_k^-$, x' and x_k^+ are decomposed into signal flip negative signal x_k^+, respectively:

$$x_k^+ = \begin{cases} x_k & x_k \geq 0 \\ 0 & x_k < 0 \end{cases} \qquad x_k^- = \begin{cases} x_k & x_k < 0 \\ 0 & x_k \geq 0 \end{cases} \tag{4}$$

The channel transmission model of wireless communication system is obtained by the above description.

2.2. Signal analysis of data transmission in wireless communication

Based on the construction of the wireless communication channel model, in order to realize the transmission of encrypted data transmission, it needs to communicate with the LFM signal encoding is designed as test signal in wireless communication transmission, LFM signal has high time frequency resolution, can effectively carry out the Doppler expansion of transmission data. In wireless communication, the output terminal, the receiving end receives the LFM signal waveform for wireless said:

$$s(t) = \cos[2\pi f_0 t + \pi \beta t^2 + \psi_0] \tag{5}$$

Wherein, f_0 and ψ_0 respectively are the space multipath channel initial frequency and initial phase. In the process of the transmitter and the receiver sends the multipath channel of wireless communication and receiving the data transmission time sequence spread spectrum can be expressed as:

$$p_{ri}(t) = p(t) * h_i(t) + n_{pi}(t) \tag{6}$$

In the formula, the propagation attenuation coefficient $h_i(t)$ is expressed, and the scanning frequency bandwidth is W. The processing gain between the wireless communication elements in the space multipath channel relative to the different paths is:

$$S_{ri}(t) = S(t) * h_i^{'}(t) + n_{si}(t) \tag{7}$$

In the model, $h_i^{'}(t)$ is the propagation attenuation coefficient of $S(t)$ transmission, and the direct sequence spread spectrum is carried out by impulse response, and the transmission coding output of wireless communication is obtained:

$$r_i^{'}(t) = S_{ri}(t) * p_{ri}(-t) = S(t) * p(-t) * h_i^{'}(t) * h_i(-t) + n_{1i}(t) \tag{8}$$

In the formula:

$$n_{1i}(t) = S(t) * h_i^{'}(t) * n_{pi}(-t) + n_{si}(t) * p(-t) * h_i(-t) + n_{si}(t) * n_{pi}(-t) \tag{9}$$

The upper formula is represented as an electromagnetic noise interference item in the wireless communication of the space multipath channel:

$$r(t) = \sum_{i=1}^{M} r_i^{'}(t) * p(t) = S(t) * p(t) * p(-t) * \sum_{i=1}^{M} h_i^{'}(t) * h_i(-t) + \sum_{i=1}^{M} n_i(t) \tag{10}$$

In the formula, $n_i(t)$ is the wireless communication between the transmission symbol high resolution receivers, it receives the intersymbol interference, expressed as $n_i(t) = n_{1i}(t) * p(t)$. in the continuous emission of a plurality of LFM signals, multipath vector recombination according to the peak position detected by $h_i(t)$ to calculate $h_i^{'}(t)$, spatial data transmission coding gain chaos, continuous detection the receiving end so as to realize the signal and the received signal copy correlation and improve the receiving directivity gain of wireless communication, according to the above analysis, the chaotic wireless communication data source encoding based on output as shown in Figure 1.

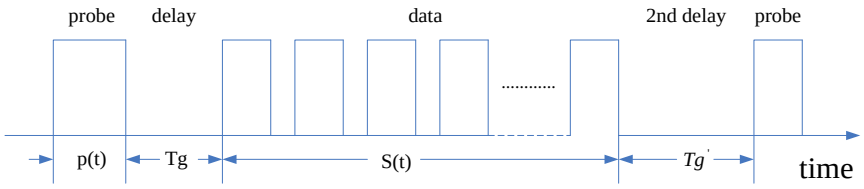

Fig. 1 Data source coding of wireless communication

3. Chaotic encryption algorithm and communication optimization

3.1. Encryption algorithm design

This paper presents an improved wireless communication technology to optimize the chaotic encryption technology based on communication data sampling in wireless communication channel model, chaotic encryption of communication signal sampling, chaotic encryption algorithm uses the Logistic mapping as the basis function, the general definition for Logistics mapping:

$$f(x) = \begin{cases} x / p, & x \in [0, p) \\ (1-x) / p, & x \in [p, 1] \end{cases} \tag{11}$$

The mapping is through the parameters of p to get the Logistics map, when GHH, the mapping for the standard Lorenz chaotic map, if it is a sequence of characters encoding, it can be extended Logistics mapping to complete the sequence of encoding symbols, ordering structure of wireless communication transmission, and its expression is:

$$f(x)=\begin{cases} x/P_1, & x\in I_1 \\ (x-P_1)/P_2, & x\in I_2 \\ \cdots\cdots & \cdots\cdots \\ (x-\sum_{i=1}^{n-1}P_i)/P_n, & x\in I_n \end{cases} \tag{12}$$

Here, $P_i(i=1,\ldots\ldots,n)$ denotes the probability of each symbol appearing in the sequence, and the interval I_i represents the cumulative probability interval

$$\sum_{i=1}^{n}P_i=1 \tag{13}$$

$$I_1=[0,P_1] \tag{14}$$

$$I_i=\left[\sum_{j=1}^{i-1}P_j,\sum_{j=1}^{i}P_j\right],i=2,3,\ldots\ldots,n. \tag{15}$$

According to the theory of source entropy, the self information of s_i is $-\log_2(P(s_i))$, and the average information of corresponding sequence is:

$$H=-\sum_{i=1}^{n}P_i\log_2(P_i) \tag{16}$$

The sequence $s=\{s_i,i=1\ldots M\mid s_i\in S\}$, where S represents the set of symbols that appear in the sequence, and the probability that each symbol appears in the s can be represented as:

$$P_n=\frac{1}{M}card\{s_i\mid s_i=S_n\} \tag{17}$$

Wherein, $S_n\in S,n=1\ldots N$. Pseudorandom sequence encoding the wireless communication chaos generated by another chaotic encryption, pseudo-random sequence generation is the key parameter and initial chaos generated by encoding the value before determined. This method improves the plaintext, correlation between encoding and encryption, the encryption and encoding form a unified whole.

3.2. Key design and chaotic encryption coding

The time reversal mirror technique is used to encrypt the chaos, and the limiting noise is introduced to obtain the weighting coefficients of the time reversal mirror:

$$\{b_1',b_2',\cdots,b_v'\}=\arg\min_{\{b_1,b_2,\cdots,b_v\}}(\max_{\sum_{v=1}^{V}b_v\bullet x_v<0,1\le n\le N}|\sum_{v=1}^{V}b_v\bullet x_v|^2) \tag{18}$$

Wherein, x' is taken on the polar decomposition, OFDM wireless communication system for signal receiver:

$$y(t)=r\bullet h(t)\otimes s(t)+z(t) \tag{19}$$

In the upper model, r is the photoelectric conversion efficiency in the wireless communication system, $s(t)$ is the transmitting signal, and the time reversal method is adopted to obtain the positive signal s_k^+ of the chaotic encryption output:

$$s_k^+=\begin{cases} V_{\max} & x_k^+>V_{\max} \\ x_k^+ & 0\le x_k^+\le V_{\max} \end{cases} \tag{20}$$

The flip negative signal of chaotic encryption s_k^- is expressed as:

$$s_k^-=x_k^-+\chi_k \tag{21}$$

While, $\tilde{y}_k^-<\gamma$ is considered as interference of wireless communication, while $\tilde{y}_k^-\ge\gamma$ is regarded as the compensation signal of wireless communication.

In order to improve the randomness of the chaotic sequence, the first 50 iterations, and then get a $\lceil r/16 \rceil$ iteration sequence value, then each sequence of values in the binarization processing for the length of the 16 binary number, the final composition of $x_1x_2x_3.....x_r$, encryption sequence required so the ciphertext sequence is obtained by encoding sequence and $c_1c_2c_3.....c_r$, bitwise $c_i = t_i \oplus x_i, i = \{1,2,.....,r\}$ encryption sequence, for each block encoding to update encryption key, updated as follows:

$$\begin{cases} KC_1 = KC_1 \oplus \{t_j, t_{j+1}, t_{j+2}, ..., t_{j+m-2}\} \\ KS_1 = KS_1 \oplus \{t_{j+m-2}\} \end{cases} \tag{22}$$

Wherein, $j = r \bmod 128$,if $j > r - m$,then $j = j - m$,if $j = 0$, $j = m$,and the remaining blocks are coded and encrypted according to the steps described above, and the encoding and encryption are completed.

Because the decoding is carried out in accordance with the block, in order to distinguish between the "011111111" block sequence into each block sequence, in order to ensure that each block sequence only one flag sequence, all 7 consecutive "1" after adding a "0".

4. Simulation experiment and result analysis

In order to test the performance of this algorithm in chaotic encryption and communication to improve the quality of wireless communication is realized in the simulation experiment. The experimental platform based on Xilinx Virtex-5, using 64Kb Block RAM floating-point data as the original test data, using 100 receiver array transmission network composed of wireless communication, the BPSK modulation signals with multipath time variable broadband characteristics, using BPSK modulation signal as the signal simulation of wireless communication system, wireless communication symbol rate is 1kBaud, the space distance between symbols is 20~29m, the array element spacing is 1m, the communication carrier frequency is 3kHz, and the communication distance is 2km, the transmit elements first launch $p(t)$, the waiting time $Tg = 100\text{ms}$, sub carrier numbers were 12 and 46, the wireless communication signal by using the space interval 4 times of sampling, set according to the simulation environment and parameters, wireless communication chaos encryption and data transmission In the simulation experiment, the transmission signal model is first given, as shown in Figure 2.

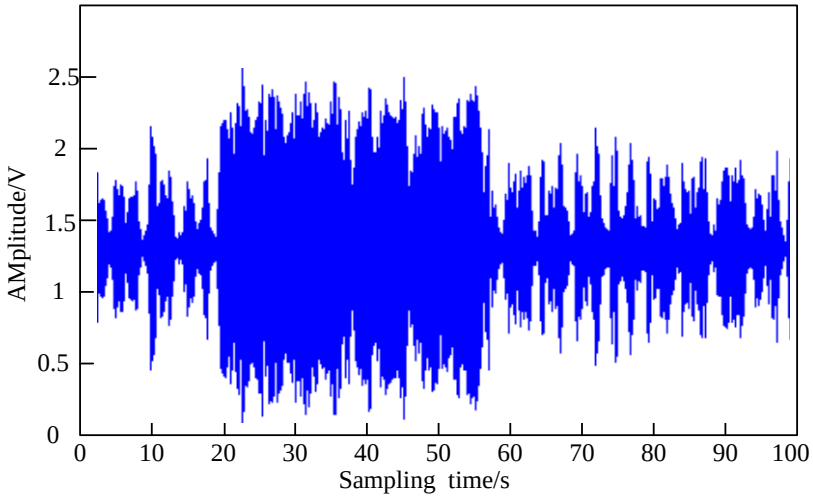

Figure 2 Wireless communication signal transmission model

Take the wireless communication signal model as the research object, chaotic encryption and encoding simulation is taken, wireless communication data encryption is divided into 50 blocks, each block size is 225 Byte, the codebook size is 1024 code vector, the encrypted signal waveform

as shown in Figure 3.

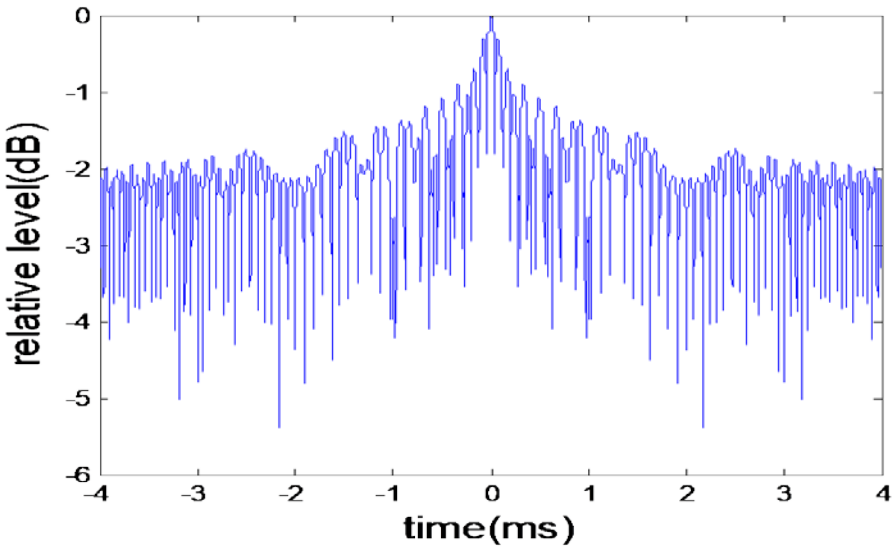

Fig. 3 Chaotic encryption coding output of wireless communication

It can be seen from the diagram, the algorithm of chaotic encryption of wireless communication data transmission, can improve the transmission capability of data confidentiality, it has good encryption performance. In table 1, encrypting communication error rate comparison results are presented with this method and traditional method. It shows that the method of encryption processing error of communication output rate is low, and it can improve the fidelity of wireless communication ability.

Tab 1 Bit error rate (%) comparison

Array elements	Chaotic	DS	MF
3	3.5	22.3	14.3
8	2.3	12.3	12.4
10	0	12.1	10.3
30	0	7.3	8.5
50	0	7.4	7.5
60	0	4.3	5.3

5. Conclusions

In order to improve the security of wireless communications and security, this paper proposes a wireless communication optimization technology based on chaotic encryption technology. The results show that the encryption process using the method of wireless communication, improve the communication security, effective Improve the fidelity of communication transmission, channel equalization performance is better, it has very good application value in wireless communication optimization.

Acknowledgements

Research on Key Technologies of Data Collection and Transmission System in Intelligent Parking Service Platform 2018A-113

References

[1] DENG Z H, CAO L B, JIANG Y Z, et al. Minimax probability TSK fuzzy system classifier: A more transparent and highly interpretable classification model[J]. IEEE Transactions on Fuzzy

Systems, 2015, 23(4): 813-826.

[2] HE Y, ZHANG C S, TANG X M, et al. Coherent integration loss due to pulses loss and phase modulation in passive bistatic radar [J]. Digital Signal Processing, 2013, 23(4):1265-1276.

[3] HAO H. Multi component LFM signal detection and parameter estimation based on EEMD-FRFT [J]. Optik-International Journal for Light and Electron Optics, 2013, 124(23):6093-6096.

[4] GOVONI M A, LI H, KOSINSKI J A. Range-Doppler resolution of the linear-FM noise radar waveform [J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(1):658-664.

[5] PAN Ying, TANG Yong, and LIU Hai. Access control in very loosely structured data model using relational databases [J]. Acta Electronica Sinica, 2012, 40(3): 600-606.