http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (9): 1673-1677, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1673.1677

A Novel Structure for Covert Communication Based on Alpha Stable Distribution

[1]Zhijiang Xu, [1]Jing Yuan, [2]Kang Wang, [1]LiMin Meng and [1]Jingyu Hua
[1]College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310023, China
[2]Zhejiang Police College, Hangzhou, 310053, China

Abstract: A novel structure of secure communication system is proposed. The alpha stable noise sequence which is used for random carrier, is modulated by the binary message sequence to achieve the purpose of secure communication in some scenarios, such as military communications. The correlation between the first and the latter half symbol period of a stable non-Gaussian noise sequence carries the binary information. The receiver of the proposed random communication system demodulates the received signal by calculating the correlation coefficient between the first and the latter half sybmol period of the transmitted noise sequence to recover the binary message sequence. The proposed communication system significantly simplifies the structure of the transceiver because only one alpha-stable noise source in the transmitter and a simple non-coherent demodulation in the receiver are required. To evaluate the proposed system, the Bit Error Rate (BER) performance under additive white Gaussian noise channel is analyzed. And simulation results show that the BER of the system is very low, thus proving that system proposed is rational and secure.

Key words: Symmetric alpha stable, covert communication, random carrier, additive white Gaussian noise channel

INTRODUCTION

The key methods for covert communication at present are the chaotic modulation and spread spectrum technology. Since the chaotic modulated carrier is non-periodic chaotic signal with broadband, pulse-like autocorrelation and low cross-correlation (Wu and Zuo, 2013), it is suitable for covert communication. However, the power of broadband chaotic signal concentrates on low-frequency components, thus greatly reducing the security of communication. The spread spectrum communication technology based on pseudo-random sequence is also a good choice for covert communication but its receiver must have all the knowledge of spread spectrum sequence and strictly synchronize with the transmitter (Dezhi *et al*., 2011). More importantly, the conventional Direct Spread Sequence Spectrum (DSSS) is easy to be detected by methods such as high order statistics method and the second-order cyclic statistics method. Therefore, its confidentiality is not strong.

In 1993, Shao and Nikias raised a research boom of α-stable distribution in the field of signal processing (Shao and Nikias, 1993). In the next ten years, researches and applications on α-stable distribution develop rapidly. In many communication channels, such as MIMO-OFDM Fading Channels, acoustic channels and the multiple access interference in a multi-user network, the observed noise exhibits non-Gaussian impulsive characteristics, e.g., the received signal is corrupted by heavy-tail distributions noise (Wang *et al*., 2012). Such kind of ambient noise can be modeled with α-stable distribution based on the generalized central limit theorem. As a consequence, a stochastic process obeying Symmetric Alpha Stable (SαS) which is modulated by the binary message bit stream, is used for the modulation carrier. Hence, the transmitted signals are similar to the ambient noise and difficult to detect. Thus, the purpose of secure communication is achieved. In addition, it can also minimize the noise pollution and limit the human impact on wildlife due to its low power transmission (Dimitrov *et al*., 2012).

In 1999, Salberg put forward to the conception of secure digital communications by means of Stochastic Process Shift Keying (SPSK) (Salberg and Hanssen, 1999). Transmit a stochastic process (noise-like) $X_0(t)$, $0<t\le T$, to represent bit '0' and another stochastic process $X_1(t)$, $0<t\le T$ to represent bit '0'. The mathematic expression for SPSK is given by:

$$S_k(t)=\begin{cases}X_0(t), & \text{if } b_k='0'\\ X_1(t), & \text{if } b_k='1'\end{cases} \quad (1)$$

where, $S_k(t)$ is the corresponding signal of the k-th bit b_k.

Corresponding Author: Zhijiang Xu, College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310023, China Tel: +8657185290372

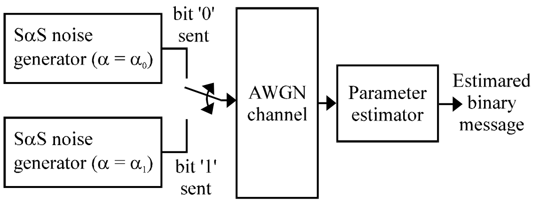

Fig. 1: Communication scheme proposed by Cek (Cek and Savaci, 2009)

This encoding scheme avoids the discontinuities in waveform. Therefore, it hides the timing information. In addition, because the transmitted signal appears noise-like, the scheme can be used for covert communication as well.

Cek M.E. proposed a new technique to achieve a covert communication system (Cek and Savaci, 2009). The block diagram of the scheme is shown in Fig. 1.

The parameter of the stable non-Gaussian noise sequence is modulated by the binary message sequence to achieve a secure communication system. The characteristic exponent 'α' of an SαS sequence carries the binary information. Specially, if the message bit is logic '0' (or respectively '1'), then the α_0-stable (or respectively α_1-stable) sequence is transmitted during the bit length T, where the α_0-stable means that the characteristic exponent of an SαS process is α_0. The receiver of the proposed communication schemes estimates the characteristic exponent of the received sequence and a hard limiter determines the sent binary message.

However, the communication scheme proposed by Cek has some disadvantages. First of all, it increases the complexity of the communication system because that the transmitter requires two different SαS noise sequence generators. Secondly, the transmitted signals with different statistical characteristics are easy to be detected when α_0 is far away α_1. Hence, the BER performance is improved while the security is worse. On the contrary, those two signals are difficult to distinguish when α_0 is close to α_1. Hence, the security is improved while the BER performance is worse. Finally, the accurate estimation of the characteristic exponent α is the key factor of the proposed scheme. Therefore, lots of samples (or the relatively long bit length T) are required to obtain the accurate estimated the α parameter. That means that the sending rate is low.

To overcome these disadvantages, a novel structure of covert digital communication system is proposed in this study. The transmitter only requires one α-stable distributed noise generator. Hence, it significantly simplifies the structure of the transmitter and reduces the probability of detection. The receiver adopts a non-coherent demodulation and avoids the problem of parameter estimation. Moreover, the performance of the proposed communication system is improved while the hardware cost is reduced.

The rest of the study is organized as follows. First of all, SαS distribution is briefly introduced. Secondly, a novel covert communication system is proposed. It employs the SαS noise sequence as noise-like carrier which is modulated by the message. In this section, the structure of the transceiver is given and then the demodulation method in the receiver is presented based on the orthogonality of the noise-like carrier. Finally, the simulation results show that the proposed covert communication system obtains a better performance with simple structure and low complexity.

SYMMETRIC ALPHA STABLE DISTRIBUTION

This section gives a brief introduction of Symmetric Alpha Stable (SαS) distribution. Levy put forward the concept of alpha stable distribution in 1925. The alpha stable distributions are able to describe various impulsive noises almost perfectly and satisfy the wide-sense center extreme limit theorem. The SαS distribution is important, since in most of the practical communication systems, the noise is assumed to be symmetrical. In particular, the Gaussian distribution can be considered as a special case of the SαS distribution. The SαS distribution can be completely determined by two parameters: (1) A characteristic exponent $\alpha \in (0, 2)$ which indicates the characteristic of the tail of the SαS distribution. Specifically, a smaller α leads to a heavier tail with the algebraic decay compared to the Gaussian distribution which decays exponentially, (2) A divergence (or scale) parameter $\sigma>0$ (or $\gamma = \sigma^\alpha$) which is analogous to the variance of the Gaussian distribution. The Probability Density Function (PDF) of the SαS distribution is yet no explicit expression, except for the Cauchy distribution ($\alpha = 1$) and the Gaussian distribution ($\alpha = 2$). However, its Characteristic Function (CF) is very simple and given by:

$$\phi(t) = \exp(-\sigma^\alpha|t|^\alpha) = \exp(-\gamma|t|^\alpha) \quad (2)$$

STRUCTURE OF THE PROPOSED TRANSMITTER

In this section, the transmitter structure is proposed, in which an alpha stable distribution sequence is used for carrier. As shown in Fig. 2, the bit length T is divided into two equal parts. The latter half is same or opposite as the first half which is decided by the binary message. Specially, if the transmitted bit is logic '0', the latter half of the transmitted signal is the same as the first half; on the

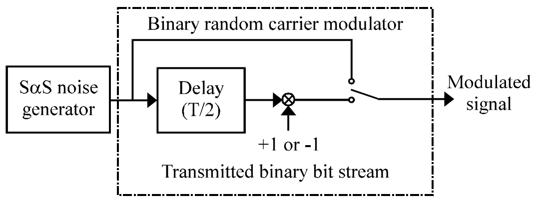

Fig. 2: Block diagram of proposed random carrier transmitter, where T is the bit length

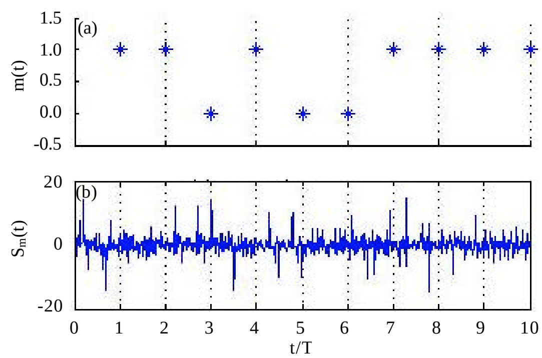

Fig. 3(a-b): Binary message bit stream m(t) vs bit length T (upper) and corresponding transmitted signal in time domain $S_m(t)$ (lower) (a) Binary bit stream and (b) Transmitted noise sequare

contrary, if the transmitted bit is logic '1', then the latter half of the transmitted signal is the opposite of the first half.

Let c(t) denote the random carrier sequence generated by the SαS noise generator in symbol period T/2 and the corresponding random carrier function g(t) is given by:

$$g(t) = c(t)[u(t)-u(t-T/2)] \tag{3}$$

where, u(t) represents an unit step function. Based on the function g(t), the close-form expression of the proposed modulated signal is given by:

$$S_m(t) = g(t)+(-1)^{m(t)}\, g(t-T/2) \tag{4}$$

where, m(t) = {0,1} is the binary message.

The transmitted noise sequence is shown in Fig. 3, together with the combined arbitrary bit stream with T = 20 and α = 1.5. The SαS distribution noise sequence has been generated by the method given in (Veillette, 2009).

STRUCTURE OF THE PROPOSED RECEIVER

This section describes the structure of the receiver. The receiver of the proposed communication scheme, as

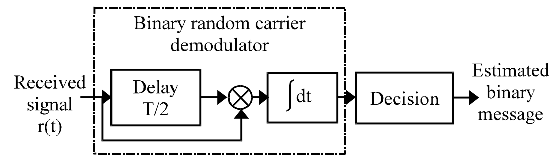

Fig. 4: Non-coherent demodulator of the proposed receiver

shown in Fig. 4, calculates the correlation function of the received noise sequence in a bit length T and a hard limiter determines the sent binary message. Without considering the channel fading and additive noise, the received signal r(t) equals the transmitted signal $S_m(t)$. For simplicity, assume that the receiver has a perfect synchronization. Let $z_m(t)$ denote the output of the demodulator which is given by:

$$\begin{aligned} z_m(t) &= \int_{T/2}^{T} r(t)r(t-T/2)\,dt \\ &= \int_0^{T/2} g(t)(-1)^{m(t)} g(t)\,dt = (-1)^{m(t)} \int_0^{T/2} c^2(t)\,dt \end{aligned} \tag{5}$$

And the decision rule is very simple, i.e., if $z_m(t)$ is larger than 0, the estimated value $\hat{m}(t)$ = 0; Conversely, if $z_m(t)$ is less than 0, $\hat{m}(t)$ = 1 is transmitted.

Non-coherent demodulation avoids the carrier recovery and synchronization problems. It also contributes to simplify the structure of the decision module which only requires a simple hard limiter.

SIMULATION RESULTS

This section demonstrates the feasibility and effectiveness of the proposed communication system under AWGN channel. Since the α-stable distributions (except Gaussian) do not have finite second moments, the variance becomes meaningless here (Ma and Nikias, 1995; Nikias and Shao, 1995). Hence, SNR is not available to measure the quality of the channel. To solve this problem, Mixed Signal-to-Noise Ratio (MSNR) is defined instead (Liu *et al*., 2009). Since in this communication system, the transmitted signal is SαS distributed noise and the channel noise is Gaussian noise, the MSNR is defined as follows:

$$MSNR_{dB} = 10\log_{10}(\gamma_s/\sigma_v^2) \tag{6}$$

where, γ_s denotes the dispersion of α-stable distributed noise and σ_v^2 denotes the variance of Gaussian noise. Since the α distributed noise employed is standard α-stable distributed, γ equals to one, i.e., γ = 1.

Figure 5 shows the transmitted signals of the system when taking α = 1.5, T = 100 and MSNR = -5 dB. The

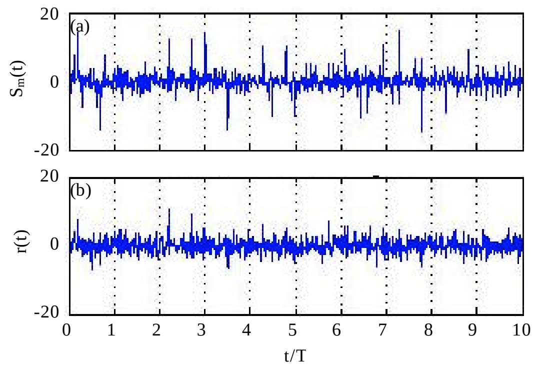

Fig. 5(a-b): Transmitted signal and the received signal (under AWGN channel): (a) Modulated signal $S_m(t)$ vs bit length T and (b) Received signal r(t) vs bit length T

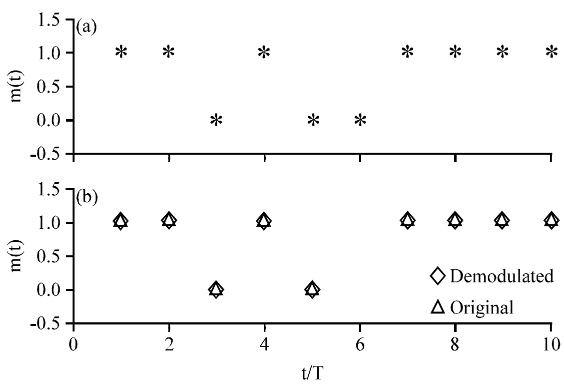

Fig. 6(a-b): Binary message m(t) (upper). For each bit length T, estimated bit value m(t) which is the output of the demodulator (lower) (a) Original bit stream and (b) Estimated bit stream

sub-figure in the upper illustrates the common transmitted signal and the sub-figure in the lower illustrates the transmitted signal with AWGN noise.

Figure 6 illustrates the original bit stream (the upper sub-figure) compared with the demodulated bit stream (the lower sub-figure). Since the demodulated bit stream is the same as the original one, the BER performance of the communication system proposed is quite good.

In order to broaden the universality of the simulation, this study performs a lot of simulations under different α and T to evaluate the performances of the proposed scheme. Assume that the number of transmitted symbols is 10000 and in each case of value the experiment is done 200 times. Taking the average, the BERs when MSNR varies from -10 to 10 dB are obtained.

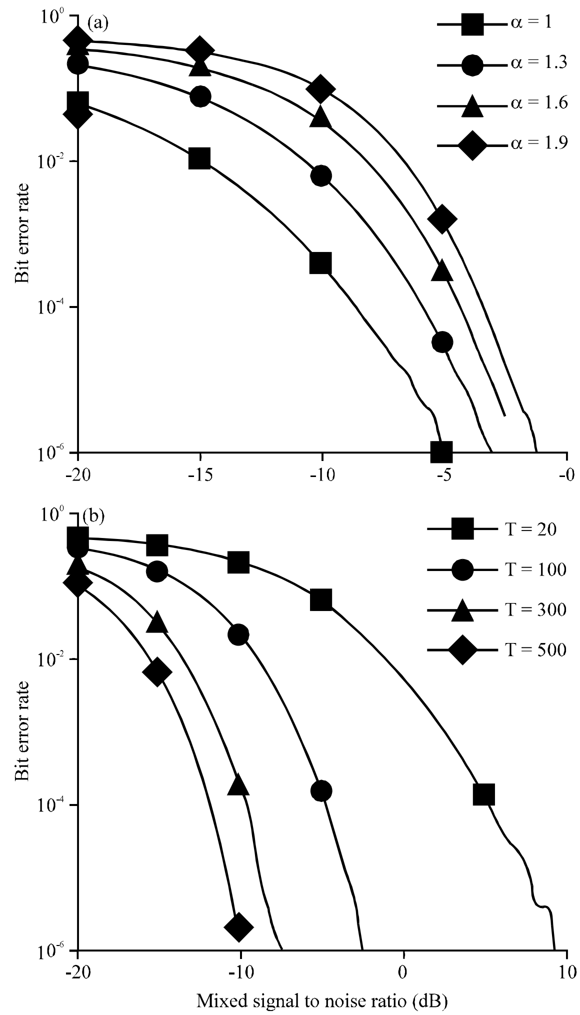

Fig. 7(a-b): Bit Error Rates vs channel MSNR under (a) Various the characteristic exponents of the alpha stable distribution and (b) The bit length T

Figure 7a shows the BERs of the proposed system when T = 100 and characteristic parameter α of the carrier are 1.0, 1.3, 1.6, 1.9, respectively. When T is fixed, with the increasing of the characteristic exponent of the alpha stable distribution, the bit error rate gradually decreases. And no matter what values T are, the BERs reduce gradually as MSNR increases.

Figure 7b shows the BERs of the proposed system when 1.5 and T are taken 20, 100, 300, 500 respectively. When the characteristic exponent α is fixed, as the bit length T increases, the BER also gradually reduces. Meanwhile, regardless of what values α are, the BERs reduce gradually as MSNR increases.

As shown in Fig. 7, the performance of the proposed system comes out to be very good. For example, in the case of α = 1.5 and T = 100, the BER of the system is below 10% when MSNR = -10 dB. This result is of great importance to covert communication, since it means that the receiver recoveries the noise-like transmitted bit stream even when transmitted power is low.

CONCLUSION

A novel structure for covert digital communication is proposed in this study which performs very well even though its structure is relatively simple. And due to the simple structure of the system, it is easy to be put into practice. Simulation results also show that under the condition of low MSNR, the BER performance of the proposed system is very good. In a word, the structure of the proposed communication system, where an alpha stable distribution sequence is used for random carrier, offers a new way for the security communication with low BER.

ACKNOWLEDGMENT

The authors would like to thank Professor Yuan Wu for his valuable and helpful comments which have improved the presentation. This material is based upon work funded by Zhejiang Provincial Key Science and Technology Innovative Team (2010R5011), Zhejiang Provincial Visiting Scholar Professional Development Project (FX2012069) and Zhejiang Provincial Key Laboratory of Communication Networks and Applications.

REFERENCES

Cek, M.E. and F.A. Savaci, 2009. Stable non-Gaussian noise parameter modulation in digital communication. Electron. Lett., 45: 1256-1257.

Dezhi, L., G. Xuemai and G. Qing, 2011. Anti-detection performance of code-hopping direct sequence spread spectrum system. Inform. Technol. J., 10: 1325-1333.

Dimitrov, K.E., J.A. Neasham, B.S. Sharif, C.C. Tsimenidis and G.M. Goodfellow, 2012. Low-power environmentally friendly underwater acoustic communication using pseudo-noise spreading sequences. Proceedings of the IEEE International Conference on Oceans, May 21-24, 2012, Yeosu, Korea, pp: 1-5.

Liu, W.H., Y.Y. Wang, B. Wang, B.Q. Huang and T.S. Qiu, 2009. Stochastic resonance based latency delay estimation for weak evoked potentials with impulsive noises. Proceedings of the 9th IEEE International Conference on Computer and Information Technology, Volume 1, October 11-14, 2009, Xiamen, China, pp: 252-257.

Ma, X. and C.L. Nikias, 1995. Parameter estimation and blind channel identification in impulsive signal environments. IEEE Trans. Signal Process., 43: 2884-2897.

Nikias, C.L. and M. Shao, 1995. Signal Processing With Alpha-Stable Distribution and Application. John Wiley and Sons Inc., New York.

Salberg, A.B. and A. Hanssen, 1999. Secure digital communications by means of stochastic process shift keying. Proceedings of the Record of the 33rd Asilomar Conference on Signals, Systems and Computers, Volume 2, October 24-27, 1999, Pacific Grove, CA., USA., pp: 1523-1527.

Shao, M. and C.L. Nikias, 1993. Signal processing with fractional lower order moments: Stable processes and their applications. Proc. IEEE, 81: 986-1010.

Veillette, M., 2009. Alpha-stable distributions in MATLAB. http://math.bu.edu/people/mveillet/html/alphastablepub.html

Wang, K., Z.J. Xu, Y. Wu and J.Y. Hua, 2012. A robust and simple piecewise approximation to SáS distribution with bi-region model. Inf. Technol. J., 11: 1121-1126.

Wu, Z. and H. Zuo, 2013. Projective synchronization for a class of unknown chaotic systems based on adaptive fuzzy control. Inf. Technol. J., 12: 214-218.