Fluctuation and Noise Letters
Vol. 16, No. 2 (2017) 1750024 (10 pages)

DOI: 10.1142/S0219477517500249

Random Communication System Based on Skewed Alpha-Stable Levy Noise Shift Keying

Areeb Ahmed* and F. Acar Savaci

Izmir Institute of Technology, Department of Electrical and Electronic Engineering, Urla 35430, Izmir, Turkey
**areebahmed@iyte.edu.tr*

Received 27 February 2017
Accepted 16 May 2017
Published 15 June 2017
Communicated by Laszlo B. Kish

The digital communication system is based on the skewed alpha-stable (α-stable) noise sequence which is chosen as the random carrier to modulate the binary message at the transmitter side. Antipodal characteristic of the skew parameter beta (β) is exploited for decoding information at the receiver side to obtain a secure communication system. A fast estimator used in this paper is based on Modified Extreme Value Method (MEVM) to extract the binary message from the signal received through the Additive White Gaussian Noise (AWGN) channel. Our proposed receiver is achieving better bit error rate (BER) versus Mixed Signal to Noise Ratio (MSNR) than previously introduced receivers which are based on Sinc and Logarithmic estimators. MEVM estimator is indeed less complex compared to the Sinc and Logarithmic estimators and hence more fast. Additionally, the criterion to measure the security level of random communication system, which is based on α-stable noise sequence, has also been introduced.

Keywords: Random communication; alpha-stable Levy noise; extreme value method.

1. Introduction

Efforts to use noise as a carrier to establish more secure or covert spread spectrum communication system started in 1950's [1]. A complete stochastic communication system based on stochastic process shift keying (SPSS) was first introduced by Salberg, and Hanssen in [2]. In their system, two different autoregressive/moving average (ARMA) processes were used to send binary messages. In [3], Cek and Savaci introduced symmetric α-stable (SαS) noise as a random carrier in their proposed random communication scheme and the characteristic exponent "α" which is the impulsiveness measure of the data has been used for encoding the binary message. A sinc estimator introduced in [4] was used in [3] to estimate the binary message from the received signal. Later on, Bit error rate (BER) of the scheme introduced in [3] was evaluated in [5]. However in [6], the random communication scheme was modified by using skewness parameter (β) of skewed α-stable noise as a random carrier and better

performance was obtained. A new model of (SαS) communication system based on a logarithmic moment estimator was introduced recently in [7]. Both sinc estimator and logarithmic estimator used in [3, 7] were first introduced by Kuruoglu in [4]. While sinc estimator is more simple and fast compared to the logarithmic estimator, however, the logarithmic estimator is more accurate in sense of BER and therefore, the choice of estimator would depend on the type of communication data. However, the newly introduced receiver in this paper uses Modified Extreme Value Method (MEVM) given in [4] to estimate the skewness parameter "β" of the tail statistics of the received signal through Additive White Gaussian Noise (AWGN) channel. MEVM which estimates "β" has been built on the Extreme Value Method (EVM) proposed in [8] where "α" is estimated. In [4], it is claimed that the EVM is the fastest among the proposed three estimators. But, the tradeoff in choosing EVM is the computational complexity and BER efficiency which depend on the sequence of length "K" and the number of segments "L" of the EVM estimator.

2. Proposed Random Communication System

In this paper, the need of having fast estimator with least complexity and BER efficiency for random communication system using skewed alpha-stable distribution has been fulfilled with MEVM estimator. BER performance with respect to the parameters $(\alpha, \beta, \gamma, \mu)$ of the skewed α-stable distribution has been simulated for the proposed random communication system. Perfect synchronization between transmitter side and receiver side is assumed in our proposed system. The proposed random communication system is shown in Fig. 1.

2.1. *Transmitter side*

The binary message sequence is taken from Bernoulli random variable that produces "1"s and "0"s with equal probability and considered as uncorrelated. However, the factor of correlation in bits to decode information is already exploited before in [5] and recently in [9]. The binary message is encoded by skewness parameter "β" of the α-stable Levy noise X which has distribution $S_\alpha(\beta, \gamma, \mu)$ "i.e., $X \sim S_\alpha(\beta, \gamma, \mu)$".

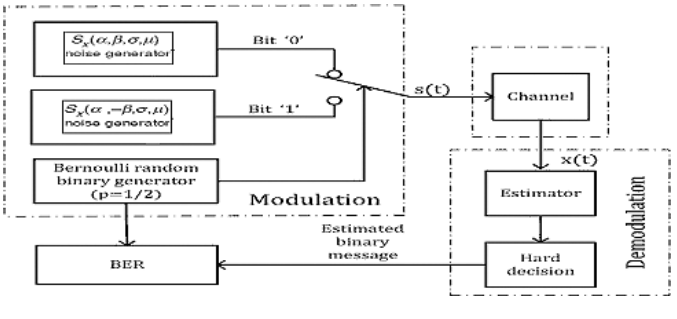

Fig. 1. Block diagram of the random communication system.

$X_0 \sim S_\alpha(\beta_0, \gamma, \mu)$ is used to code message signal "0" and $X_1 \sim S_\alpha(\beta_1, \gamma, \mu)$, where $\beta_1 = -\beta_0$ is used to code message signal "1".

The characteristic function of α-stable Levy noise $X \sim S_\alpha(\beta, \gamma, \mu)$ having α-stable distribution is expressed as

$$\phi(\theta) = \begin{cases} \exp\left\{ j\mu\theta - \gamma^\alpha |\theta|^\alpha \left(1 - j\beta \text{sign}(\theta) \tan\left(\frac{\alpha\pi}{2}\right)\right)\right\} & \text{if } \alpha \neq 1, \\ \exp\left\{ j\mu\theta - \gamma|\theta| \left(1 + j\beta \frac{2}{\pi} \text{sign}(\theta) \ln\left(\frac{\alpha\pi}{2}\right)\right)\right\} & \text{if } \alpha = 1, \end{cases} \tag{1}$$

where the parameters are defined in the respective ranges as the characteristic exponent α $(0 < \alpha \leq 2)$, the skewness parameter $\beta(-1 \leq \beta \leq 1)$, the dispersion parameter γ $(\gamma \geq 0)$ and the location parameter $\mu \in R$, in [10, 11]. Gaussian Noise is a special α-stable distribution with $\alpha = 2$. Also, choosing $\alpha < 2$ is a necessary requirement to have infinite variance in α-stable distribution to generate a shot-noise like process. Additionally, $\alpha \leq 1$ can be chosen to have undefined mean as well in α-stable distribution as mentioned in [10, 11]. Duration length of the samples x_0 and x_1 are denoted by T_b. N represents the number of noise samples per information bit and T_b is the duration for the consecutive noise samples and hence T_bN is the duration needed to encode single message bit. In Fig. 2, the binary message sequence and the corresponding transmitted noise sequence with $T_b = 1$ and $N = 1000$ are shown. The noise sequence which has skewed α-stable Levy noise has been generated by the method given in [12]. Because of the infinite variance of skewed α-stable noise for $\alpha < 2$; few large amplitude samples can only be observable in the transmitted noise sequence in the bottom part of Fig. 2 with the scale of 10^7.

2.2. *Receiver side*

The receiver is based on estimating the skewness parameter of the received signal from AWGN channel by MEVM Estimator given in [4]. The method proceeds by

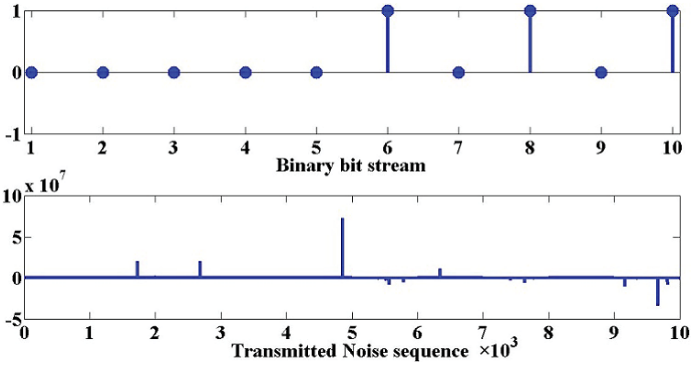

Fig. 2. Binary message sequence (Top), Transmitted Signal in time (Bottom); Bit length $T_b = 1$, $N = 1000$ noise samples per information bit, $T_bN = 1 \times 10^3$.

subdividing the received data $\{x_1, x_2, \ldots, x_N\}$ in duration $T_b N$ consisting of N samples into L non-overlapping segments of length K (i.e., $K = N/L$). The logarithms of the maximum and minimum samples from each segment l (where $l = 1, 2, \ldots, L$) from total L segments are then computed and denoted by $Y_{l\max}$ and $Y_{l\min}$.

$$Y_{l\max} = \log\{\max(x_{lk-k+i} | i \in 1, 2, \ldots, K)\}, \tag{2}$$

$$Y_{l\min} = \log\{-\min(x_{lk-k+i} | i \in 1, 2, \ldots, K)\}. \tag{3}$$

The sample means and corresponding variances of $Y_{l\max}$ and $Y_{l\min}$ and Estimates for β are then obtained as

$$Y_{\max} = \frac{1}{L}\sum_{l=1}^{L} Y_{l\max}; \quad s^2_{\max} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{l\max} - Y_{\max})^2, \tag{4}$$

$$Y_{\min} = \frac{1}{L}\sum_{l=1}^{L} Y_{l\min}; \quad s^2_{\min} = \frac{1}{L-1}\sum_{l=1}^{L}(Y_{l\min} - Y_{\min})^2, \tag{5}$$

$$\hat{\beta} = 1 - \frac{2}{\exp(\hat{\alpha}(S_{\max} - S_{\min}))}, \quad \text{where } \hat{\alpha} = \frac{\pi}{2\sqrt{6}}\left(\frac{1}{Y_{\max}} + \frac{1}{Y_{\min}}\right) \tag{6}$$

and the binary message is estimated using hard decision.

2.2.1. *Bias in MEVM estimator*

MEVM estimator "$\hat{\beta}$" is not an unbiased estimator of β as mentioned in [4, 8]. The bias of the MEVM estimator $\hat{\beta}$ increases as alpha approaches to two (Gaussian case). Otherwise, it is capable of giving estimates close to maximum likelihood (ML) estimates as mentioned in [4, 8]. Additionally, the bias of the MEVM estimator "$\hat{\beta}$" can be kept under control if large data sets (N) and number of segments (L) are used as proven in [8, Table 2]. And it can be seen in our results, that due to the utilization of large "L and N", our proposed approach is giving good performance in the sense of BER.

2.2.2. *Complexity and fastness of MEVM estimator*

In [7], it was explained that the logarithmic estimator is faster compared to the sinc estimator. The sinc estimator is much complex because it requires the calculation of absolute and signed fractional moments and inversion of sinc function each time for decoding a single binary bit.

However, the logarithmic estimator also requires equating sample moments and the actual moments and then we may solve for the characteristic exponent and skewness parameter using the third-order moment for decoding a single binary bit which is considered as a drawback [4].

Whereas, the simplicity of the MEVM estimator can be seen in (2–6) which requires the calculation of simple mean and variances of the observed data each time.

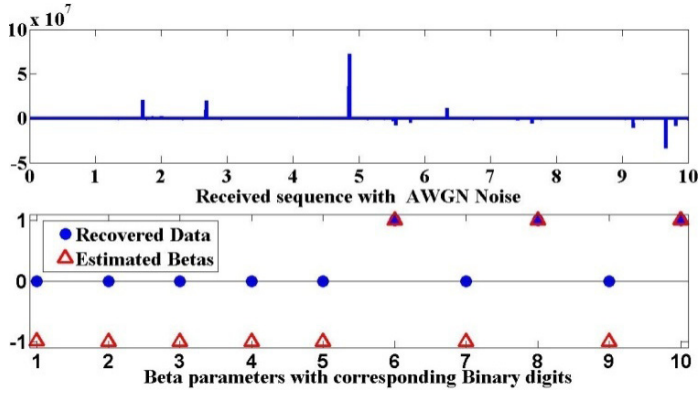

Fig. 3. Received signal from AWGN channel in time domain (Top), estimated beta parameters and recovered binary message (Bottom); bit length $T_b = 1$, $N = 1000$ noise samples per information bit, $T_b N = 1 \times 10^3$.

It decreases the amount of computation and lessons the overall complexity of the receiver. Hence, it is claimed as fast estimation approach than sinc and logarithmic estimators by Kuruoğlu in [4].

The received noise sequence through AWGN channel and the estimated beta parameters together with the corresponding estimated binary message have been shown in Fig. 3.

3. Simulation

The length and number of segments termed as "K and L" are very crucial factors and they determine the computational complexity level of our newly proposed receiver. MEVM has never been used before in the receiver to optimize BER performance and to maximize or minimize the computational complexity of the receiver in random communication systems. The minimum number of segments and the length of segments $L_{\min}$ and $K_{\min}$, respectively, are at least equal to two and the maximum number of segments and length of segments $L_{\max}$ and $K_{\max}$ are at most equal to $\frac{N}{2}$ (i.e., $L_{\min} = K_{\min} = 2$ and $L_{\max} = K_{\max} = \frac{N}{2}$).

3.1. *Performance criterion*

In Fig. 4, BER versus MSNR performance of our proposed receiver has been shown where Mixed Signal to Noise Ratio (MSNR) or Dispersion Ratio (DR) are defined as in [13] while BER is the percentage of bits with errors divided by the total number of bits that have been transmitted.

$$\mathrm{MSNR}_{\mathrm{dB}} = 10 \log \frac{\gamma}{\gamma_G}, \tag{7}$$

where γ and γ_G are the dispersion parameters of the information bearing α-stable random signal and the channel noise, respectively. It can be clearly seen that our

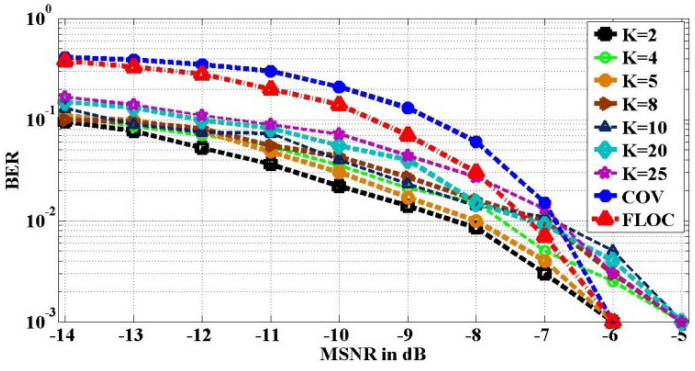

Fig. 4. BER versus MSNR (dB) with different "L and K" of estimator in AWGN channel; transmitted bits = 1000; where $\alpha = 1.6$; (where $\beta_1 = -\beta_0 = 1$).

newly proposed receiver is outperforming the receivers based on covariance method (COV) and fractional lower-order covariance method (FLOC) proposed in [5, 6], respectively. Additionally, it is giving better BER for various values of "K" of MEVM estimator hence resulting in various choices of complexity level. Also, better BER can be obtained for $\alpha < 1.6$.

3.2. *Security performance tradeoff characteristics (SPTC)*

Random communication schemes always face a classical tradeoff problem of balancing between an acceptable BER and the possibility of interceptors to decode our message, but no criterion has been introduced yet to reflect it. The scheme can be defined as the random communication system for a specific impulsiveness parameter "α" and MEVM estimator parameters "L and K". In the sequel, the SPTC for determining the security of the proposed random communication scheme based on the following definitions have been newly introduced.

Definition 1. Security parameter "$\Delta\beta$"
Security parameter $\Delta\beta$ is used to obtain the security performances of the schemes and is defined as

$$\Delta\beta \triangleq \beta_1 - (-\beta_0). \tag{8}$$

Definition 2. Security level S_L
S_L is the required security level chosen by the users for the percentage of security required and it lies within $0 \leq S_L \leq 1$.

Definition 3. Security boundary function B (.)
SPTC can give an optimal boundary based on the Security Boundary function which can be considered as a BER function with respect to the security parameter "$\Delta\beta$" and is denoted by $B(\Delta\beta)$ and lies with in $0 \leq B(\Delta\beta) \leq 1$.

For the chosen S_L, the security boundary function B (.) has been constructed from the following iterative relation given below in (9):

$$B(\Delta\beta^{(k+1)}) = B(\Delta\beta^{(k)}) \cdot \Delta\beta^{(k+1)} \cdot (1 - S_L), \tag{9}$$

where

$$\Delta\beta^{(k)} = (0.2) \cdot k, \quad k = 0, 1, \ldots, 10, \quad 0 \leq \Delta\beta^{(k)} \leq 2$$

with initial condition $B[\Delta\beta^{(0)}] = 1$ which is actually the achievable Maximum BER for the random communication system.

Definition 4. Strength of the security boundary S_{sb}
S_{sb} is the sum of all BER's obtained from the security boundary function with respect to the corresponding $\Delta\beta^{(k)}$ of the security boundary, i.e.,

$$S_{\text{sb}} = \sum_k B_{S_L}(\Delta\beta^{(k)}), \tag{10}$$

where $B_{S_L}(.)$ corresponds to security boundary function $B(.)$ for the specific security level S_L. This is actually approximation of the area under the B (.)

$$S_{\text{sb}} \cong \frac{1}{0.2} \int_{k=0}^{10} B_{S_L}(\Delta\beta) \cdot (\Delta\beta). \tag{11}$$

Definition 5. Strength of the scheme S_s
S_s is the sum of all values obtained from $B_s(.)$ with respect to corresponding $\Delta\beta^{(k)}$ for that specific scheme.

$$S_s = \sum_k B_s(\Delta\beta^{(k)}), \tag{12}$$

where $B_s(.)$ corresponds to the function which gives BER for the specific scheme at each $\Delta\beta^{(k)}$.

Definition 6. Secure scheme
The schemes whose $B_s(.)$ lie above the security boundary $B_{S_L}(.)$ are not secure while the schemes whose $B_s(.)$ lie below the security boundary B_{S_L} (.) are considered as secured as shown in Fig. 5.

Since some of the schemes intersect the security boundary, they cannot be classified according to the above definition. Therefore, the following definition for such schemes has been given below.

Definition 7. Cost of any scheme "C_s"
The Cost of a scheme "C_s" can be calculated to determine the security especially for those schemes which are intersecting the security boundary.

$$C_s \triangleq S_s - S_{\text{sb}}. \tag{13}$$

Negative cost indicates secure scheme and positive cost indicates vulnerable scheme. The absolute value of the C_s indicates either more secure or more vulnerable scheme.

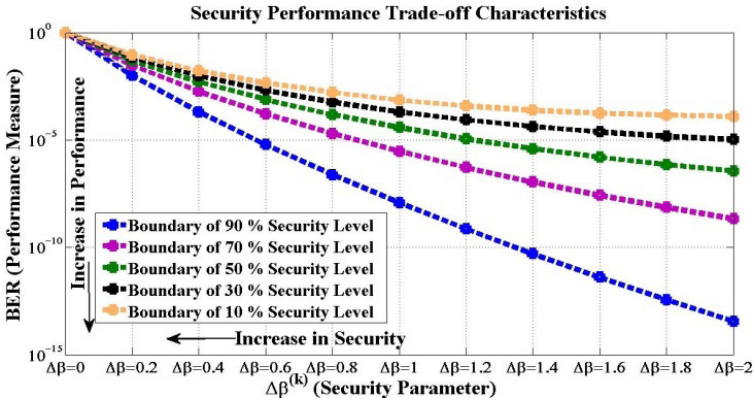

Fig. 5. BER versus security parameter ($\Delta\beta$) with different S_L.

SPTC with security boundaries "B_{S_L} (.)" for all security levels "S_L" obtained from the above security boundary function B (.) as given in (9) is shown in Fig. 6.

The results based on the above criteria for our system have been shown in Fig. 6. The increase in $\Delta\beta$ (i.e., the increase in the differences of the skewness of the noise distributions of the related binary messages) results in better BER. By decreasing the $\Delta\beta$ makes it difficult for an eavesdropper to decode the binary message since the amount of positive and negative samples for the corresponding binary messages is getting almost equal (i.e., the distributions of the coresponding binary messages are more similar). Therefore, in Fig. 5, $\Delta\beta$ is also labeled as "security parameter" on x-axis while the BER on y-axis is labeled as "performance measure". The increase in the impulsiveness of the noise data (i.e., decrease in "α") would result in the heavy tail of the corresponding noise distribution used to encode the binary message. Hence, making it easy for the MEVM estimator to estimate the beta parameters from

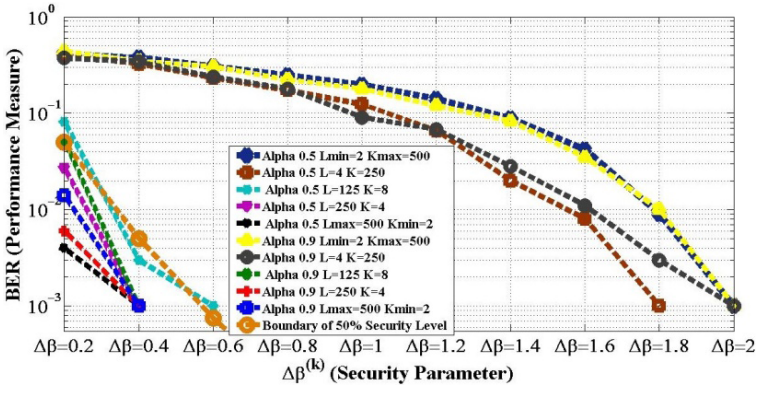

Fig. 6. BER versus security parameter ($\Delta\beta$) with different "α" parameters and "L and K" of estimator; transmitted bits = 1000; $S_L = 0.50$.

Table 1. Cost of different schemes for their corresponding strengths.

	Name of scheme	S_{sb}	S_s	C_s
$\alpha = 0.5$	$L_{\min} = 2$ $K_{\max} = 500$	0.0559	1.1862	1.1303
	$L = 4$ $K = 250$	0.0559	0.7334	0.6775
	$L = 125$ $K = 8$	0.0559	0.0180	−0.0379
	$L = 250$ $K = 4$	0.0559	0.0058	−0.0501
	$L_{\max} = 500$ $K_{\max} = 2$	0.0559	0.0084	−0.0475
$\alpha = 0.9$	$L_{\min} = 2$ $K_{\max} = 500$	0.0559	1.1020	1.0460
	$L = 4$ $K = 250$	0.0559	0.7346	0.6787
	$L = 125$ $K = 8$	0.0559	0.0108	−0.0451
	$L = 250$ $K = 4$	0.0559	0.0124	−0.0435
	$L_{\max} = 500$ $L_{\max} = 2$	0.0559	0.0032	−0.0527

the mixture of AWGN noise (i.e., $\alpha = 2$) and the transmitted α-stable noise (i.e., $\alpha \neq 2$) which results in better BER. While the decrease in impulsiveness of the noise data will make the system more secure by mixing the samples of the transmitted signal for the corresponding binary message extremely close to the samples of AWGN channel.

The cost of all schemes "C_s" for their coresponding S_s have been given in Table 1. As mentioned earlier, the schemes whose BER's are below the security boundary have their costs in negative and hence more secure. Also, the scheme like "$\alpha = 0.5$, $L = 125$, $K = 8$" whose BER's intersect the security boundary has negative cost. So, the scheme "$\alpha = 0.5$, $L = 125$, $K = 8$" can be considered as secured which cannot be known without C_s just by looking at Fig. 6.

Increment in L or decrement in K increases the computational complexity and vice versa. So, accuracy and complexity tradeoff would depend on the type of communication data.

4. Conclusion

Our proposed receiver based on MEVM estimator for the skewed α-stable distribution shift keying is fast and outperforms the receivers based on COV and FLOC given in the literature. Our proposed receiver also introduces the advantage of variable computational complexity and performs extremely well based on the newly introduced security criterion "SPTC" to compare the random communication systems which are based on α-stable noise parameter modulation. The effects of imperfect synchronization on our proposed system are left open issue for further work.

Acknowledgments

The authors wish to acknowledge all the comments and suggestions made by the reviewers, which clearly improved the technical content of the paper, as well as the clarity in its presentation.

References

[1] B. L. Basore, Noise-like signals and their detection by correlation, Ph.D. thesis, MIT, Cambridge, MA (1952).

[2] A. B. Salberg and A. Hanssen, Secure digital communications by means of stochastic process shift keying, in *Proc. Int. Conf. Signals, Systems, and Computers* (PacificGrove, USA, 1999), pp. 1523–1527.

[3] M. E. Cek and F. A. Savaci, Stable non-Gaussian noise parameter modulation in digital communication, *IET Electron. Lett.* **45**(24) (2009) 1256–1257.

[4] E. E. Kuruoğlu, Density parameter estimation of skewed alphastable distributions, *IEEE Trans. Signal Process.* **49**(10) (2001) 2192–2201.

[5] Z. Xu, J. Yuan, K. Wang, L. Meng and J. Hua, A novel structure for covert communication based on alpha stable distribution, *Inform. Technol. J.* **13** (2014) 1673–1677.

[6] M. E. Cek, Covert communication using skewed α-stable distributions, *IET Electron. Lett.* **51**(1) (2015) 116–118.

[7] Z. J. Xu, K. Wang, Y. Gong, W. D. Lu and J. Y. Hua, Structure and performance analysis of an SαS-based digital modulation system, *IET Commun.* **10**(11) (2016) 1329–1339.

[8] G. A. Tsihrintzis and C. L. Nikias, Fast estimation of the parameters of alpha-stable impulsive interference, *IEEE Trans. Signal Process.* **44** (1996) 1492–1503.

[9] Z. Xu, Y. Gong, K. Wang, W. Lu and J. Hua, A covert digital communication system based on joint normal distribution, *IET Commun.* (2017).

[10] G. Samorodnitsky and M. S. Taqqu, *Stable Non-Gaussian Random Processes* (Chapman & Hall/CRC, 1994).

[11] D. Applebaum, *Levy Processes and Stochastic Calculus* (Cambridge University Press, New York, 2004).

[12] A. Janicki and A. Weron, *Simulation and Chaotic Behaviour of A-Stable Stochastic Processes* (Marcel Dekker, New York, 1994).

[13] W. H. Liu, Y. Y. Wang, B. Wang, B. Q. Huang and T. S. Qiu, Stochastic resonance based latency delay estimation for weak evoked potentials with impulsive noises, *Ninth IEEE Int. Conf. Computer and Information Technology*, 2009, Xiamen, pp. 252–257.