IET Communications

Research Article

ISSN 1751-8628
Received on 25th July 2018
Revised 14th August 2019
Accepted on 5th November 2019
E-First on 5th March 2020
doi: 10.1049/iet-com.2018.5702
www.ietdl.org

Inverse system approach to design alpha-stable noise driven random communication system

Ferit Acar Savaci[1], *Areeb Ahmed*[1] ✉

[1]*Department of Electrical and Electronic Engineering, Izmir Institute of Technology, Urla 35430, Izmir, Turkey*

✉ *E-mail: areebahmed@iyte.com.tr*

Abstract: In the proposed random communication system (RCS), the alpha-stable (α-stable) noise as a random carrier drives the transmitter which is modelled by the linear dynamical system and the skewness parameter of the random carrier encodes the binary messages. By selecting the receiver as the inverse system of the transmitter, the output of the receiver is ensured to be α-stable noise whose skewness parameters are then estimated to decode the binary messages. The response of a linear system to an α-stable process is again α-stable process, however, the skewness parameters of the response differs from that of the input which can only be recovered at the output of the inverse system. Hence, estimation of skewness parameter by an eavesdropper, without using the inverse system, will not reveal the true binary messages while the intended receiver truly decodes the binary messages. The proposed inverse system based RCS provides efficient performance which is shown by comparing the bit error rate of the intended receiver and an eavesdropper where the enhancement in covertness is shown by evaluating the covertness values of the proposed RCS.

1 Introduction

Physical layer security of digital communication systems is considered as a key factor in ensuring covert transmission. The thought to exploit alpha-stable (α-stable) noise as a random carrier to employ physical layer secured communication system started in 2009 [1]. However, attempts to use skewed α-stable (SkαS) distributed noise as a random carrier or building SkαS distributed noise-based communication systems, i.e. random communication systems (RCSs), to achieve the required purpose began in 2015 [2]. The bit error performance (BER) for the introduced binary shift keying based RCSs in [1, 2], was later evaluated in [3] which proves the practicality of the idea. Later on, M-ary RCS introduced in [4] provided further motivation to design more efficient RCSs. Therefore, different receiver have also been utilised to enhance the performance of RCSs [5]. However, the most optimised model of the RCS based on SkαS Levy noise shift keying (Sk-αSNSK) has been introduced in [6]. Similarly, synchronised RCS was recently introduced in [7] as the first method for synchronisation of RCSs.

In RCSs, decoding the received signal is impossible without knowing the pulse length, i.e. duration of a single binary information bit. However, it is shown in [8] that if the exact pulse length can be found then it would be possible for an eavesdropper to retrieve the binary messages hidden in the transmitted α-stable noise signals by one of the estimation methods given in [9]. Therefore, the true level of covertness cannot be assured in the previously proposed RCSs [1–7].

In this paper, the newly developed RCS, as shown in Fig. 1, includes the mth-order linear time invariant (LTI) dynamical system with Sk-αSNSK signal generator (SG) at the transmitting end ‘Alice’ while the intended receiver ‘Bob’ uses the inverse LTI dynamical system of the transmitter with the modified extreme value method (MEVM)-based estimator. As a result, the parameters needed to decode the information carrying α-stable input has been increased from single parameter, i.e. pulse length, to the state parameters of the utilised LTI dynamical system as well. The bit error rate (BER) performances of Bob and an eavesdropper ‘Willie’ reflects that Willie is unable to retrieve the hidden binary messages even if he knows the pulse length, as he is not aware of the state parameters of the LTI system used by Alice. In comparison to Willie, Bob is achieving more efficient BER performance as expected from any covert communication system. Similarly, the criterion to quantify the covertness of the proposed RCS, introduced in [8], has been utilised to analyse the security of the proposed RCS. The covertness analysis reflects that the utilisation α-stable noise driven inverse system can significantly increase the covertness of RCSs.

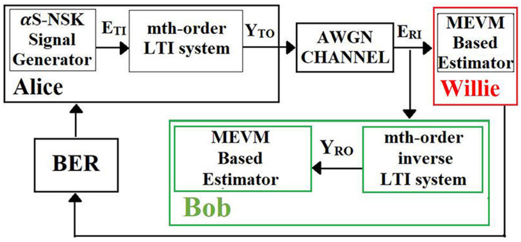

Fig. 1 *Block diagram of the proposed RCS based on the inverse system*

The inspiration to use linear inverse dynamical system in the context of RCS has come through the steps: (i) the analytical results obtained in [10] says that the skewness parameter of the output of LTI system changes in terms of the transfer function of the LTI system and the skewness and scale parameters of α-stable random input; (ii) hence, at the transmitter's output, the skewness parameter of the transmitter's input cannot be decoded, therefore estimating the skewness parameter of the transmitter's input is only possible at the corresponding inverse system's output. In the sequel, α-stable noise is briefly introduced and then the transmitter and the receiver shown in Fig. 1 are presented.

2 Alpha-stable noise and distribution

The α-stable noise can be generated by α-stable distribution. $S_\alpha\,(\beta, \gamma, \mu)$ denotes the distribution of α-stable noise ‘E’, i.e. $E \sim S_\alpha\,(\beta, \gamma, \mu)$; where the characteristic exponent ‘α’ which determines the impulsiveness of noise lies in the interval $(0, 2]$, the skewness parameter ‘β’ lies in the interval $[-1, 1]$, ‘γ’ and ‘μ’ are the dispersion (scale) and the location parameters, respectively [11]. The α-stable distribution can be generated by the method given in [12] by the characteristic function of α-stable noise $X \sim S_\alpha\,(\beta, \gamma, \mu)$ expressed in [11] as

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

Note: $X \sim S_{\alpha=2}$ $(\beta = 0, \gamma, \mu)$, $X \sim S_{\alpha=1}$ $(\beta = 0, \gamma, \mu)$ and $X \sim S_{\alpha=0.5}$ $(\beta = 1, \gamma, \mu)$ denotes Gaussian, Cauchy and Levy Distributions, respectively as they are special cases of α-stable distributions.

Remark: the α-stable distribution does not have a second or higher order moments for $\alpha < 2$, moreover, the first order moment does not also exist for $\alpha \leq 1$ [11].

3 System description

The considered RCS model consists of the transmitter 'Alice', intended receiver 'Bob' and an eavesdropper 'Willie'.

3.1 Alice (transmitter)

The transmitter consists of Sk-αSNSK SG and a second-order LTI system. The Sk-αSNSK SG generates random noises E_{TI_1}, i.e. $E_{\mathrm{TI}_1} \sim S_{\alpha}$ $(-\beta_{\mathrm{TI}}, \gamma_{\mathrm{TI}}, \mu)$, and E_{TI_2}, i.e. $E_{\mathrm{TI}_2} \sim S_{\alpha}$ $(\beta_{\mathrm{TI}}, \gamma_{\mathrm{TI}}, \mu)$ to encode the binary messages '0' and '1', respectively, by exploiting the antipodal characteristics of SkαS distribution; where β_{TI} equals to 1 or −1 have been used to represent the distribution skewed to the right or to the left, respectively, $\Delta\beta \triangleq \beta_{\mathrm{TI}} - (-\beta_{\mathrm{TI}})$ is the difference between the two β_{TI} used for encoding the binary message '0' and '1'. The duration needed to encode a single binary message bit is $T_{\mathrm{b}}N$, i.e. the pulse length; where T_{b} is the length of a single noise sample and N is the number of generated noise samples to encode a single binary message bit represented as $\{e_{\mathrm{TI}_1}, e_{\mathrm{TI}_2}, \dots, e_{\mathrm{TI}_N}\}$.

The signals generated from the Skα-SNSK SG are then applied to the transmitter which is mth-order LTI dynamical system containing m state variables, p inputs and q outputs, represented as $\mathscr{R} = [\boldsymbol{A}\ \boldsymbol{B}\ \boldsymbol{C}\ \boldsymbol{D}]$ in [8]; where $\boldsymbol{A} \in R^{m \times m}$, $\boldsymbol{B} \in R^{m \times p}$, $\boldsymbol{C} \in R^{q \times m}$ and $\boldsymbol{D} \in R^{q \times p}$. In the proposed RCS, we have chosen the representation $\boldsymbol{A} = \begin{bmatrix} 0.98 & -0.01 \\ -0.01 & 0.98 \end{bmatrix}$, $\boldsymbol{B} = \begin{bmatrix} -0.06 \\ 2.19 \end{bmatrix}$, $\boldsymbol{C} = [0 \quad -0.16]$, and $\boldsymbol{D} = [-0.33]$ which yielded the best BER performance for the intended receiver among the many arbitrary selected system representations $\mathscr{R}$s and their corresponding inverse systems. Moreover, the sub parameters of $\mathscr{R} = [\boldsymbol{A}\ \boldsymbol{B}\ \boldsymbol{C}\ \boldsymbol{D}]$, i.e. the values of the elements of the matrices $\boldsymbol{A} \in R^{m \times m}$, $\boldsymbol{B} \in R^{m \times p}$, $\boldsymbol{C} \in R^{q \times m}$ and $\boldsymbol{D} \in R^{q \times p}$, have been randomly obtained by trying different combinations within the range $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$ ϵ [−1, 3]. The parameters of the system $\mathscr{R} = [\boldsymbol{A}\ \boldsymbol{B}\ \boldsymbol{C}\ \boldsymbol{D}]$ are pre-determined and known only to the transmitter and to the intended receiver in a similar way the transmitter and the intended receiver pre-decides the pulse length before transmission [1–8]. As it is proven in [10] that the output of $\mathscr{R} = [\boldsymbol{A}\ \boldsymbol{B}\ \boldsymbol{C}\ \boldsymbol{D}]$ to an α-stable input is also α-stable, i.e. the input $E_{\mathrm{TI}} \sim S_{\alpha}$ $(\beta_{\mathrm{TI}}, \gamma_{\mathrm{TI}}, \mu)$ results in the output $Y_{\mathrm{TO}} \sim S_{\alpha}$ $(\beta_{\mathrm{TO}}, \gamma_{\mathrm{TO}}, \mu)$; where E_{TI} and Y_{TO} represent the input and output of the transmitter $\mathscr{R}$, respectively. However, the fact that $\beta_{\mathrm{TI}} \neq \beta_{\mathrm{TO}}$, as proven in [10], assures that the binary messages encoded by the skewness parameter of the input could not be truly estimated by an eavesdropper even if he is perfectly synchronised with the transmitter and knows the pulse length as well.

The arbitrary binary message stream consisting of five binary information bits with the corresponding generated α-stable noise sequence E_{TI} consisting of $E_{\mathrm{TI}_1}, E_{\mathrm{TI}_2}, \dots, E_{\mathrm{TI}_5}$ and the transmitted α-stable noise sequence Y_{TO} are shown in Fig. 2; where $\alpha = 1.5$, $\beta_{\mathrm{TI}} = 1$, $\gamma_{\mathrm{TI}} = 1$ and $\mu = 0$ are used to generate E_{TI}.

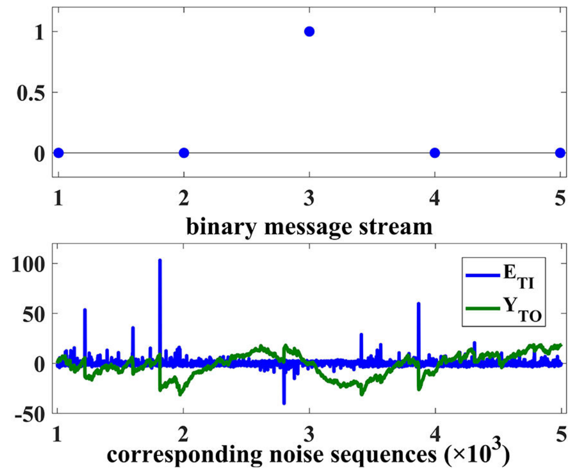

Fig. 2 *Binary messages by Alice (upper), generated and transmitted noise sequences by Alice in time domain (lower); $T_b = 1$, $N = 1000$, $T_bN = 1 \times 10^3$*

3.2 Bob and Willie (intended receiver and eavesdropper)

The α-stable noise sequence at the input of the receiver is $E_{\mathrm{RI}} = Y_{\mathrm{TO}} + G$, which is accessible to Bob and also to Willie; where the additive white Gaussian noise in the channel is $G \sim S_{\alpha_G = 2}(\beta = 0, \gamma_{\mathrm{G}} = 1, \mu = 0)$. Since, Bob is aware of the transmitter '$\mathscr{R}$' he can design his receiver as the inverse system of $\mathscr{R}$ as given in [13], i.e. $\mathscr{R}_I = [\boldsymbol{A} - \boldsymbol{B}\boldsymbol{D}^{-1}\boldsymbol{C}\ \ \boldsymbol{B}\boldsymbol{D}^{-1}\ \ -\boldsymbol{D}^{-1}\boldsymbol{C}\ \boldsymbol{D}^{-1}]$. By applying the received sequence E_{RI} to his receiver $\mathscr{R}_I$, Bob can estimate the skewness parameter $\hat{\beta}_{TI}$ from his output Y_{RO} by subdividing the received data $\{y_{\mathrm{RO}_1}, y_{\mathrm{RO}_2}, \dots, y_{\mathrm{RO}_N}\}$ holding a single binary message bit, consisting of N samples during the pulse length $T_{\mathrm{b}}N$, into $L = 25$ non-overlapping segments of length $K = 40$ (i.e. $K = N/L$). The logarithms of the maximum and minimum samples from each segment $l = 1,2, \dots, L$ from total L segments are calculated and represented below by $Y_{l-\max}$ and $Y_{l-\min}$ as

$$Y_{l-\max} = \log\{\ \max\ (y_{\mathrm{RO}lK-K+i} | i \in 1, 2,\ \dots,\ K)\} \tag{2}$$

$$Y_{l-\min} = \log\{-\ \min\ (y_{\mathrm{RO}lK-K+i} | i \in 1, 2,\ \dots,\ K)\} \tag{3}$$

The means, i.e. $Y_{\max}$ and $Y_{\min}$, and corresponding variances, i.e. $s_{\max}^2$ and $s_{\min}^2$, of the received data are then computed which is followed by an estimate for β_{TI}, i.e. $\hat{\beta}_{\mathrm{TI}}$, to decode a single binary message bit as '0' '1' if $\hat{\beta}_{\mathrm{TI}} < 0$ $(\hat{\beta}_{\mathrm{TI}} \geq 0)$.

$$Y_{\max} = \frac{1}{L}\sum_{l=1}^{L} Y_{l-\max} \tag{4}$$

$$Y_{\min} = \frac{1}{L}\sum_{l=1}^{L} Y_{l-\min} \tag{5}$$

$$s_{\max}^2 = \frac{1}{L-1}\sum_{l=1}^{L} (Y_{l-\max} - Y_{\max})^2 \tag{6}$$

$$s_{\min}^2 = \frac{1}{L-1}\sum_{l=1}^{L} (Y_{l-\min} - Y_{\min})^2 \tag{7}$$

Therefore,

$$\hat{\beta}_{\mathrm{TI}} = 1 - \frac{2}{\exp(\hat{\alpha}(S_{\max} - S_{\min}))} \tag{8}$$

where

$$\hat{\alpha} = \frac{\pi}{2\sqrt{6}}\left(\frac{1}{Y_{\max}} + \frac{1}{Y_{\min}}\right) \tag{9}$$

Even though there is not any method, algorithm or attack to crack the hidden pulse length, i.e. T_bN, of $E_{\rm RI}$ or $Y_{\rm RO}$ but considering the worst case scenario, we have assumed that both Bob and Willie know $T_{\rm b}$ and N. Therefore, Willie could also utilise the same MEVM based estimator, explained above in (2–9), to retrieve the binary message stream by estimating $\hat{\beta}_{\rm TI}$ but from the data $\{e_{{\rm RI}_1}, e_{{\rm RI}_2}, \ldots, e_{{\rm RI}_N}\}$ of the received signal $E_{\rm RI}$ while Bob is estimating from $Y_{\rm RO}$. The received noise sequences $E_{\rm RI}$ and $Y_{\rm RO}$, respectively, utilised by Bob and Willie with their retrieved binary message streams and the corresponding estimated skewness parameters, have been shown in Fig. 3.

4 Experimental results

The performance of the proposed inverse system-based RCS has been examined in this section by comparing the BER performances of Bob and Willie and the covertness has been analysed according to the only available measure of covertness for RCS proposed in [8].

4.1 BER performance analysis

It has been shown in Fig. 3 that the transmitted binary message stream is irretrievable from the $\hat{\beta}_{\rm TI}$ estimated by an eavesdropper. However, in order to accurately evaluate the proposed RCS, the BER performances of Bob and Willie have also been computed, as shown in Fig. 4, against the channel mixed signal to noise ratio (MSNR); where MSNR is defined in [9] as

$$\mathrm{MSNR}_{\rm dB} = 10\log\frac{\gamma_{\rm TI}}{\gamma_{\rm G}} \tag{10}$$

According to the BER performances of Bob and Willie, as shown in Fig. 4, for the chosen L and K, one can conclude that the intended receiver will always outperform an eavesdropper by a large BER margin, for the same value of the impulsiveness parameter 'α' utilised by Alice where BER margin is the difference between the BER of Bob and Willie at some specific MSNR for the same value of α utilised by Alice to generate the noise sequences.

Among the previously proposed RCSs in [1–6], the RCS introduced in [6] is the most optimised model till now as it has achieved comparatively better BER performance among its peers for any specific α [6, Fig. 4]. In comparison with the RCS introduced in [6], the proposed inverse system based RCS has also achieved similar BER performance while it provides a significant increase in covertness which has been shown in the next section. The BER performance degrades for higher values of α when it gets closer to that of the Gaussian noise, i.e. $\boldsymbol{\alpha}_{\rm G} = 2$, present in the channel and vice versa. Moreover, as shown in [6], much more efficient performance is expected when the greater values of L are utilised.

4.2 Covertness analysis

To analyse the security of proposed inverse system based RCS, the only criterion available is covertness value '$C_{\rm V}$' which quantifies the covertness of α-stable noise based RCSs, hence, provides a clear representation to differentiate the covertness achieved from various models of RCSs. $C_{\rm V}$ has been defined in [8] as

$$C_{\rm V} = \sum_i P_{\rm E}(i) \tag{11}$$

where $P_{\rm E}(i)$, i.e. $0 \le P_{\rm E}(\delta_i) \le 1$, computed in [8] as

$$P_{\rm E}(\delta_i) = \frac{\mathrm{BER}_{\rm W}(\delta_i)}{\mathrm{BER}_{\rm B}} \tag{12}$$

is the *ith* probability of an eavesdropper 'Willie' to decode the transmitted binary information bits with respect to synchronisation errors 'δ_i' where '$\mathrm{BER}_{\rm B} = 1/\,n$' is the BER of Bob and $\mathrm{BER}_{\rm W}(\delta_i)$ is the *ith* BER of an eavesdropper Willie 'for the corresponding *ith* synchronisation error 'δ_i' and lies with in $1/\,n \le \mathrm{BER}_{\rm W}(\delta_i) \le 1$ (where 'n' is the total number of transmitted binary message bits by Alice).

Remark: As $C_{\rm V}$ becomes higher, the covertness of RCS increases. In contrast, $C_{\rm V}$ close to zero implies less covert RCS. The absolute $C_{\rm V}$ indicates either more covert or more vulnerable RCS.

In order to analyse the covertness of the proposed inverse system based RCS, it has been compared with the most optimised model of RCS introduced in [6]. However, the covertness of the optimised model of RCS proposed in [6] has already been analysed in [8] according to the criterion given above in (11–12). Therefore, in this section of the paper, the covertness of the proposed inverse system based RCS has been evaluated and compared to the results given in [8].

For the same values of α and $\Delta\beta$ utilised by Alice in this study and in [8], the covertness value $C_{\rm v}$, as shown in Fig. 5, for the newly proposed inverse system based RCS has increased significantly in contrast to the $C_{\rm v}$ for optimised model of RCS, as shown in [8, Fig. 3]. The increase in $C_{\rm v}$ is not just for some specific value α and $\Delta\beta$ but utilising the inverse system approach to design RCS has increased the overall covertness for the complete range of parameter values which shows the usefulness and benefit of adopting inverse system approach for RCSs.

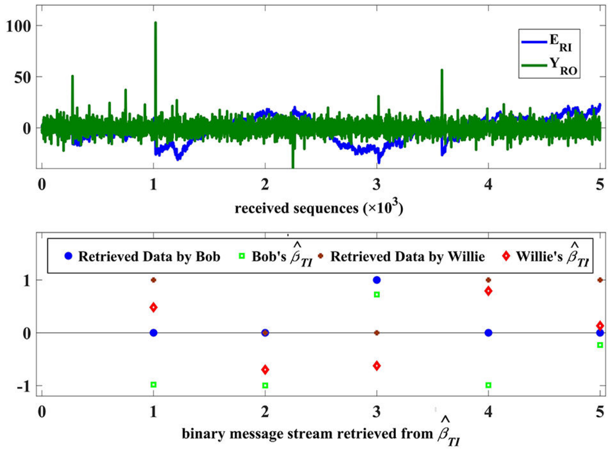

Fig. 3 *Received signals from AWGN channel in time domain (upper), estimated skewness parameters and retrieved binary messages by Bob and Willie (lower); $T_b = 1$, $N = 1000$, $T_bN = 1 \times 10^3$*

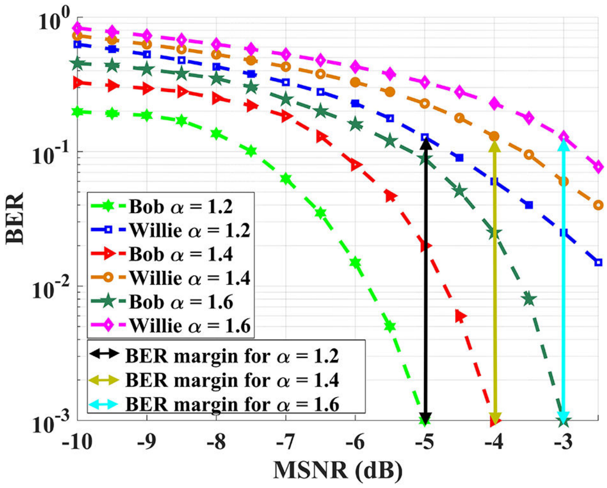

Fig. 4 *BER versus MSNR (dB) performances of Bob and Willie for the different α's utilised by Alice; number of transmitted bits = 1000*

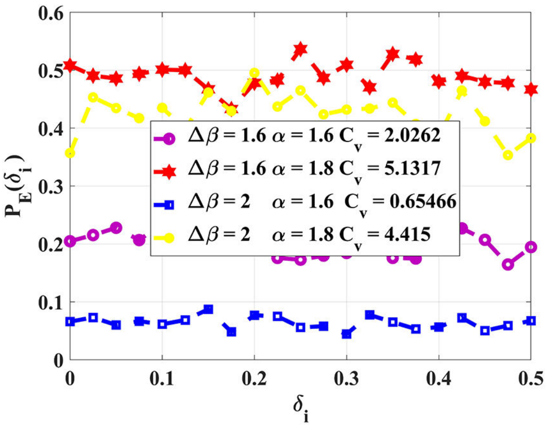

Fig. 5 *Covertness of Alice and Bob's SkαS-NSK based RCS*

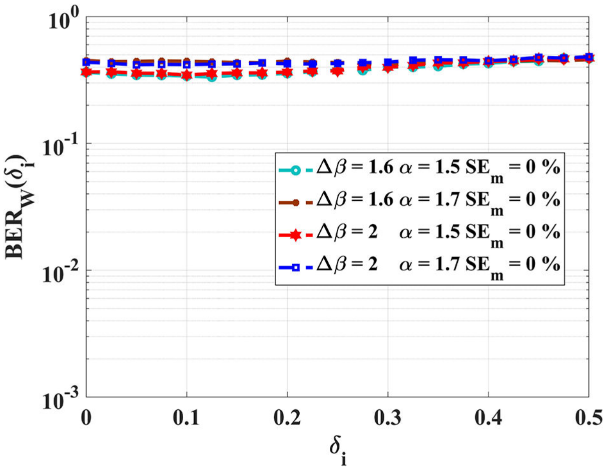

Fig. 6 *Performance of an eavesdropper Willie*

The sudden rise in C_V is due to the fact that inverse system approach results in the worst BER performance of eavesdropper Willie, i.e. $\mathrm{BER_W}(\delta_i)$, which has been evaluated and shown in Fig. 6. In comparison to the covertness analysis of optimised model of RCS in [8, Fig. 2], the performance of an eavesdropper has decreased drastically if the newly proposed inverse system based RCS is used by the transmitter and the intended receiver. Moreover, the eavesdropper is not even able to achieve the BER of 10^{-1} in the proposed inverse system based RCS.

Similarly, synchronisation error margin denoted by ‘$\mathrm{SE_M}$’ is another valueable criterion to check the vulnerability of RCSs. $\mathrm{SE_M}$ is the *ith* synchronisation error ‘δ_i’ when the BER function ‘i.e. $\mathrm{BER_W}(\delta_i)$ ‘ of Willie initially drops by $1/n$ in the range $0 \le \delta_i \le 1$ which is defined in [8] as

$$\mathrm{SE_M} = \delta_i \Big| \mathrm{BER_W}(\delta_i) < \frac{1}{n} \tag{13}$$

It has also been shown in Fig. 6 that $\mathrm{SE_M}$ available to the eavesdropper Willie has also decreased to zero which further reflects the amount of security achieved by deploying inverse system based RCSs.

5 Conclusion

The covertness of the previously proposed RCSs has been built solely on the hidden pulse length which is required for the decoding process, however, this letter presents the new RCS where the transmitter is a LTI dynamical system driven by α-stable noise which acts as a random carrier and the output of the inverse system of the transmitter is the input to the MEVM estimator for the intended receiver. According to the BER results of Bob and Willie, the intended receiver achieves significantly better performance compare to the previous RCSs. As the security complexity has been increased due to the utilisation of the inverse system, therefore the security analysis shows much bigger covertness values for the proposed RCS in comparison to the previously proposed models which reflects the enhances security level of the proposed inverse system based design.

Moreover, using higher-order LTI systems might provide more security and enhanced BER performance which will be investigated as future work.

Currently, the proposed system is only for wire communication system. However, RCSs can also be applied for wireless communication systems. As in practice, the noise cannot be directly transmitted itself. Therefore, as a pre-processing, it must be transformed into bandlimited noise. The robustness against interference and compatibility with wireless communication systems would require further signal design techniques involving filtering and modulation process for stable noise in order to restrict it within a specified bandwidth. There are the subjects of the ongoing study.

6 Acknowledgments

The authors will welcome the comments and suggestions made by the reviewers, which can improve the technical content of the paper, as well as clarity in its presentation.

7 References

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

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

[3] Xu, Z.J., Yuan, J., Wang, K., *et al.*: ‘A novel structure for covert communication based on alpha stable distribution’, *Inf. Technol. J.*, 2014, **13**, (9), pp. 1673–1677

[4] Cek, M.E.: ‘M-ary alpha-stable noise modulation in spread-spectrum communication’, *Fluct. Noise Lett.*, 2015, **14**, (3), p. 1550022

[5] Xu, Z.J., Wang, K., Gong, Y., *et al.*: ‘Structure and performance analysis of an SαS-based digital modulation system’, *IET Commun.*, 2016, **10**, (11), pp. 1329–1339

[6] Ahmed, A., Savaci, F.A.: ‘Random communication system based on skewed alpha-stable levy noise shift keying’, *Fluct. Noise Lett.*, 2017, **16**, (3), p. 1750024

[7] Ahmed, A., Savaci, F.A.: ‘Synchronisation of alpha-stable levy noise-based random communication system’, *IET Commun.*, 2018, **12**, (3), pp. 276–282

[8] Ahmed, A., Savaci, F. A.: ‘Measure of covertness based on the imperfect synchronization of an eavesdropper in random communication systems’. 10th Int. Conf. on Elec. and Elec. Eng. (ELECO), Turkey, November 2017, pp. 638–641

[9] Kuruoglu, E.E.: ‘Density parameter estimation of skewed α-stable distributions’, *IEEE Trans. Signal Process.*, 2001, **49**, (10), pp. 2192–2201

[10] Grigoriu, M.: ‘Linear systems subject to non-Gaussian *α*-stable processes’, *Probabilistic Eng. Mech.*, 1995, **10**, (1), pp. 23–34

[11] Samorodnitsky, G., Taqqu, M.S.: ‘*Stable non-Gaussian random processes*’ (Chapman & Hall/CRC, New York, USA, 1994)

[12] Janicki, A., Weron, A.: ‘*Simulation and chaotic behaviour of a-stable stochastic processes*’ (Marcel Dekker, New York, USA, 1994)

[13] Kailath, T.: ‘*Linear systems*’, vol. **156**, (Prentice-Hall, Englewood Cliffs, NJ, 1980)