Measure of covertness based on the imperfect synchronization of an eavesdropper in Random Communication Systems

Areeb Ahmed[1], F.Acar Savaci[1]

[1]Izmir Institute of Technology, Department of Electrical and Electronic Engineering, Izmir, Turkey
areebahmed@iyte.com.tr, acarsavaci@iyte.com.tr

Abstract

Random Communication Systems (RCSs) given in the literature have assumed perfectly synchronized transmitter and receiver. However in this paper, instead of assuming perfect synchronization approach in RCSs, the effects of imperfect synchronization (IS) on Skewed Alpha-Stable Noise Shift Keying (SkαS-NSK) based RCS have been observed through simulations. The Bit Error Rate (BER) performance of the eavesdropper with respect to his synchronization error in SkαS-NSK based RCS, has been analyzed. An expression for the probability of an eavesdropper to decode the binary information (i.e., Eavesdropping Probability) in SkαS-NSK based RCS, has been derived. The criterion (i.e., Covertness Value) to measure the covertness level of RCSs has also been proposed. The BER performance of an eavesdropper provides an approximate margin of synchronization error if it can be overcome by an eavesdropper then he can achieve the decoding (i.e., eavesdropping) process.

1. Introduction

Synchronization not only plays a key role in establishing successful communication link between transmitter and receiver but it also helps in boosting the performance in all types of communication systems. Especially, in Spread Spectrum (SS) based communication systems IS has a huge impact on the performance. As the average BER which is the basic performance measure in digital communication systems, the efforts to analyze the impact of IS on BER started to gain attention at the beginning of 1970's [1]. However in [2], a comprehensive analysis for the impact of IS on single carrier Direct Sequence Spread Spectrum (DS-SS) communication system was performed in which the expressions for the upper and lower bound of BER were also derived. In [3], an accurate analytical model for Overloaded Direct Sequence Code Division Multiple Access (DS-CDMA) system under IS was presented. Moreover in [4], the multi-tone (i.e., multi-carrier) DS-SS communication systems were also examined by changing the synchronization parameter. So, the factor of IS has been investigated in all types of spread spectrum based communication systems.

Also in collaborative communication, in which a number of wireless transmitters collaboratively transmit the same message signal to the common target receiver, the effects of imperfect frequency and phase synchronization were also monitored to increase the BER performance in [5, 6].

Similarly in Power Systems (PSs), the time synchronization sensors known as "Phasor Measurement Units" were analyzed for imperfect phase synchronization to improve the PS's state estimation performance in [7].

Likewise in neural communication networks, which have interconnected group of nodes in the vast network of neurons in the brain, the factor of average synchronization time error has also been used to analyze the security of cryptographic methods in [8].

Random Communication System is newly evolving branch of Spread Spectrum based covert communication. Stochastic processes are utilised as random carrier in RCS to transmit and receive binary signals in more secure way in comparision to the conventional communication systems. Salberg *et al* introduced the concept of stochastic process shift keying by utilising autoregressive/moving average (ARMA) processes as random carrier to transmit and receive binary messages [9]. Similarly, Cek *et al* initiated Symmetric alpha-Stable (SαS) noise as a random carrier to convey binary messages in [10]. After that, an approach to utilise skewed alpha-stable (SkαS) noise as a carrier was also introduced by Cek in [11]. However, the Bit error rate (BER) analysis of the proposed approaches in [9, 10] was carried out by Zhijiang *et al* in [12]. Later on, different receiver designs were also proposed in [13-14] by utilising SαS and SkαS noise as carriers to improve the BER performance. Moreover, a covert communication system based on Joint Normal Distribution has also been introduced by Zhijiang *et al* in [15]. Recently, an optimised model of RCS based on SkαS-NSK along with the first Security Performance Trade-off Characteristics to measure the security of RCS's have been introduced by Ahmed *et al* in [16]. All previous investigations on RCS's have assumed perfect synchronization between the transmitter "Alice" and the receiver "Bob". However, no approach has been proposed yet to evaluate the covertness of the RCS's in the presence of an eavesdropper "Willie" with synchronization uncertainty.

Since true level of covertness cannot be guaranteed by utilizing a stochastic process as a random carrier and assuming perfect synchronization scenario between Alice and Bob, therefore in this paper, we have evaluated the covertness of the SkαS-NSK based RCS by analyzing the BER performance of an eavesdropper "Willie" who imperfectly synchronizes with the transmitter "Alice" and tries to decode (eavesdrop) the binary information. Therefore, an expression known as "Eavesdropping Probability" is introduced to calculate the probability of Willie to successfully decode the binary information which is not transmitted covertly by Alice. Moreover, the covertness level of the SkαS-NSK based RCS, used by Alice and Bob to communicate secretly, is also evaluated by the derived expression known as "Covertness value". The BER performance of Willie also provides an approximate margin of synchronization error, own by Alice and Bob to covertly communicate by using SkαS-NSK based RCS and should be

overcome by Willie to successfully continue the hacking process.

2. System Model

The SkαS-NSK based RCS's transmitter and Modified Extreme Value Method (MEVM) based receiver for covert communication between Alice and Bob has been originally proposed by Ahmed *et al* in [16] and that work has been modified, as shown in Fig. 1, to observe the presence of an eavesdropper Willie and compute his BER performance. Similarly, the covertness level of the modifed SkαS-NSK based RCS can also be evaluated now on the basis of Willie's BER performance due to his uncertain knowledge about the synchronization method used by Alice and Bob.

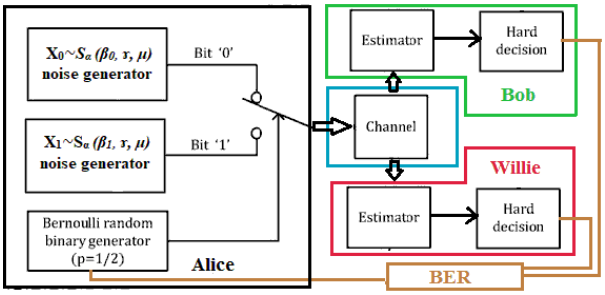

Fig. 1. *Block diagram Modified SkαS-NSK based RCS*

2.1. Alpha stable (α-stable) Distribution [17]:

α-stable noise is denoted by "S_α (β, ɤ, μ)" and the characteristic function of α-stable noise X "i.e., X ~ S_α (β, ɤ, μ)" is expressed as

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

where the ranges of the parameters are as: the characteristic exponent α ($0 < \alpha \leq 2$), the skewness parameter β($-1 \leq \beta \leq 1$), the dispersion parameter γ ($\gamma \geq 0$) and the location parameter $\mu \in R$ where α-stable stable distributions has been generated by the method given in [18].

2.2. Alice and Bob's Noise Shift Keying based RCS:

In the proposed modified SkαS-NSK based RCS, shown in Fig. 1, the binary message sequence has been taken from Bernouli Random Variable with equal probability for "1"s and "0"s. Alice is transmitting the binary message sequence encoded as $X_0 \sim S_\alpha$ (β_0, ɤ, μ) for binary information bit "0" and $X_1 \sim S_\alpha$ (β_1, ɤ, μ) for binary information bit "1" by utilising the antipodal characteristics of the skewness parameter β to skew the distributions to the right (i.e., $\beta_1 = \beta \in R^+$) or to the left (i.e., $\beta_0 = -\beta$) *as* $\beta_1 = -\beta_0$. Different parameter values for delta beta ($\Delta\beta$) "i.e., $\Delta\beta \triangleq \beta_1 - (-\beta_0)$" and α can be used to transmit the binary information bits X_0 and X_1.

Bob estimates the corresponding β and α by the Modified Extreme Value Method based receiver proposed in [16]. Since, Bob knows the exact time instant of accepting the noise samples for truly decoding binary information bits by acheiving perfect synchronization.

2.3. Eavesdropper 'Willie' in Noise Shift Keying based RCS:

It is assumed that the intended receiver "Bob" and the eavesdropper "Willie" uses the same receiver proposed in [16]. Additionally, it is also assumed that both of them knows the transmitted duration or length of a single noise sample denoted by " T_b", transmitted number of noise samples per binary information bit denoted by *"N"* and duration needed to decode single binary information bit denoted by "T_s" (i.e., $T_s = T_b N$). Bob is assumed to be perfectly synchronized with Alice and knows the exact time instant to accept the noise samples for the corresponding first binary information bit. However, Willie has no knowlege of the exact time instant to accept the noise samples for the corresponding binary information bits therefore Willie would face a synchronization error which would result in increased BER.

3. Approach to Measure Covertness

Apart from the choice of stochastic processes as random carrier, the actual method to obtain synchronization between Alice and Bob in RCS is still an open issue. Therefore in this paper, we have focused on investigating how the imperfectly synchronized Willie can influence the modified SkαS-NSK based RCS used by Alice and Bob.

Assuming that, we have a synchronization error denoted by δ in the range $0 \leq \delta \leq 1$ and Alice has transmitted the binary information bits as logic '101….', then the corresponding noise sequences "S_α (β_1, ɤ, μ), S_α (β_0, ɤ, μ), S_α (β_1, ɤ, μ)....." have been transmitted. Since Willie is imperfectly synchronized with Alice and have no knowledge of the exact time instant to accept the noise samples for the corresponding initial transmitted binary information bit 1, Willie would wrongly receive totally N samples of which (1- δ) N samples are from the distribution S_α (β_1, ɤ, μ) *(i.e.,* $x_i \sim S_\alpha$ (β_1, ɤ, μ)*)* and δN samples are from the other distribution S_α (β_0, ɤ, μ) *(i.e.,* $y_i \sim S_\alpha$ (β_0, ɤ, μ)*)* in the duration T_s which is represented as below

$$\{x_1 \ldots\ldots x_{(1-\delta)N}, y_1 \ldots\ldots y_{\delta N}\} \quad (2)$$

Similarly for the second transmitted binary message bit '0', the Willie will again wrongly receive total N samples of which (1- δ) N samples are from the distribution S_α (β_0, ɤ, μ) *(i.e.,* $y_i \sim S_\alpha$ (β_0, ɤ, μ) and δN samples are from the other distribution S_α (β_1, ɤ, μ) *(i.e.,* $x_i \sim S_\alpha$ (β_1, ɤ, μ)*)* which is represented as below

$$\{y_1 \ldots\ldots y_{(1-\delta)N}, x_1 \ldots\ldots x_{\delta N}\} \quad (3)$$

On the contrary, Bob is perfectly synchronized with Alice and knows the exact time instant to accept the noise samples for all corresponding transmitted binary information bits. Hence, he will receive the transmitted binary information bits as '101.....' which was originally sent by Alice. Therefore, Bob would face negligible or ideally erratic bits while Willie would face

increased BER with respect to the variation in the synchronization error "δ".

3.1. Performance of an Eavesdropper:

The *i-th* BER of an eavesdropper Willie denoted by "$BER_W(\delta_i)$" for the corresponding *i-th* synchronization error 'δ_i' is considered as a BER function with respect to the synchronization errors *"δ_i"* which lies with in $\frac{1}{n} \leq BER_W(\delta_i) \leq 1$ (where 'n' is the total number of transmitted binary message bits by Alice).

The $BER_W(\delta_i)$ also provides an approximate margin of synchronization error, own by Alice and Bob to covertly communicate by using SkαS-NSK based RCS.

3.2. Performance of the Intended Receiver:

Since there is no synchronization error between Alice and the intended receiver 'Bob' therefore the BER of Bob, denoted by "BER_B", has been practically considered equal to $\frac{1}{n}$.

3.3. Eavesdropping Probability 'P_E':

The *i-th* probability of an eavesdropper 'Willie' to decode the transmitted binary information bits with respect to synchronization errors δ_i is named as "Eavesdropping Probability" denoted by "$P_E(i)$" and it is defined as

$$P_E(\delta_i) = \frac{BER_W(\delta_i)}{BER_B} \quad (4)$$

which lies with in $0 \leq P_E(\delta_i) \leq 1$.

3.4. Covertness Value 'C_V':

The criterion to measure the covertness of the RCS used by Alice and Bob is named as "Covertness Value" denoted by " C_V " which is defined below as

$$C_V = \sum_i P_E(i) \quad (5)$$

The RCS used by Alice and Bob would be considered as covert as big the C_V. On the contrary, C_V close to zero implies less covert RCS. The absolute C_V indicates either more covert or more vulnerable RCS which can be used to analyze the covertness level.

3.5. Synchronization Error Margin 'SE_M':

The synchronization error margin denoted by "SE_M" is the *i-th* synchronization error 'δ_i' when the BER function "i.e., $BER_W(\delta_i)$" of Willie initially drops by $\frac{1}{n}$ in the range $0 \leq \delta_i \leq 1$ which is defined below as

$$SE_M = \delta_i \mid BER_W(\delta_i) < \frac{1}{n} \quad (6)$$

4. Simulation Results and Discussion

Simulation results for the covertness analysis of Alice and Bob's SkαS-NSK based RCS in the presence of an eavesdropper Willie, in accordance to the proposed criteria, has been done in this section. One thousand bits (i.e., *n = 1000*) has been used in simulations to obtain BERs. Different values of Δβ and α have been used to obtain results so that best parameters values can be found which should be recommended to Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

In Fig. 2, the BER performance of an eavesdropper Willie "$BER_W(\delta_i)$" with respect to all possible synchronization errors "δ_i", are shown. The increases in the differences of the skewness of the noise distributions of the related binary information bits (i.e., increase in Δβ) by Alice has resulted in better $BER_W(\delta_i)$. The distributions of the corresponding binary messages are more similar (i.e., decrease in Δβ) by Alice has worsened the $BER_W(\delta_i)$ since the amount of positive and negative samples for the corresponding binary information bits are getting almost equal. Therefore, small value for Δβ is recommended for Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

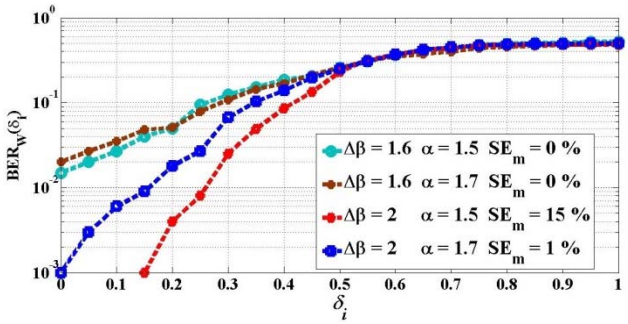

Fig. 2. *Performance of an eavesdropper Willie*

On the contrary, decrease in α by Alice would result in the heavy tail of the corresponding noise distribution used to encode the binary information bits hence making it easy for the MEVM based receiver to estimate the beta parameters from the mixture of AWGN noise in the channel *(i.e., α =2)* and the transmitted α-stable noise *(i.e., $\alpha \neq 2$)* which has resulted in better $BER_W(\delta_i)$. Therefore, higher value of α ($\alpha \to 2$) is recommended for Alice to covertly communicate with Bob when using SkαS-NSK based RCS.

The resulted SE_M's for corresponding combinations of Δβ and α in Alice and Bob's SkαS-NSK based RCS has also been shown in Fig. 2. It has been observed that Willie has less margin of synchronization error when Alice and Bob are using SkαS-NSK based RCS with small Δβ and higher α. Therefore from the resulted values of SE_M's in Fig. 2, the recommendation for Alice and Bob is to utilise smaller value for Δβ and higher value for α, when using SkαS-NSK based RCS.

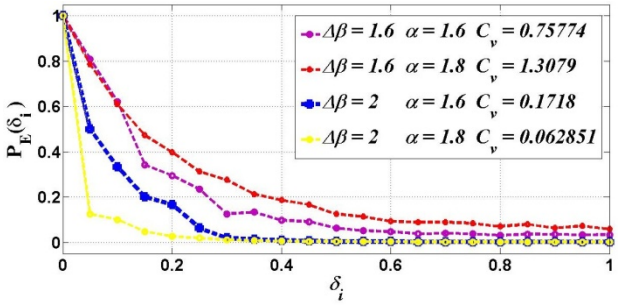

Fig. 3. *Covertness of Alice and Bob's SkαS-NSK based RCS*

Based on the performance of an eavesdropper Willie, the eavesdropping probability "$P_E(i)$" with respect to all possible synchronization errors "δ_i" is shown in Fig. 3. The covertness level (i.e., C_V) of Alice and Bob's SkαS-NSK based RCS is also shown in Fig. 3. It is seen that Willie can decode the binary information successfully even with synchronization error up to some extent, if large $\Delta\beta$ and smaller α is used by Alice to communicate with Bob in RCS. Therefore Alice and Bob should select small $\Delta\beta$ and higher α in SkαS-NSK based RCS.

5. Conclusion

We have revisited SkαS-NSK based RCSs in the presence of an imperfectly synchronized eavesdropper. The eavesdropper probability and covertness value have been proposed to measure the covertness level in the presence of an eavesdropper who has no knowledge of synchronization method used by transmitter Alice and intended receiver Bob. The SkαS-NSK based RCS shows promising results against eavesdropping with respect to synchronization errors if the recommended parameters values are used.

The impulsiveness and skewness parameters of α-stable noise can be maneuver on the transmitter side to improve the overall covertness level of SkαS -NSK based RCS which is a benefit of using α-stable noise as a carrier. Moreover, the optimum values for the impulsiveness and skewness parameters can be found by using the introduced criteria which can help Alice and Bob to communicate covertly when using SkαS -NSK based RCS. The parameters also help to achieve the desired anti covert probability and covertness value for the SkαS -NSK based RCS. The effects of different noises as carriers in RCS's on eavesdropper probability and covertness value in different channels has left open issue for further investigation.

6. References

[1] J.J. Stiffler, "Theory of Synchronous Communications", Prentice-Hall, Englewood Cliffs, New Jersey, 1971.

[2] B. M. Todorovic, "The impact of imperfect code synchronization on bit error rate in DS-SS systems: upper and lower bound", in *Electrotechnical Conference, 1989. Proceedings. 'Integrating Research, Industry and Education in Energy and Communication Engineering',* Lisbon, *MELECON.,* 1989, pp. 524-527.

[3] S. Jos, P. Kumar, S. Chakrabarti, "An Accurate Analytical Model for Overloaded DS-CDMA under Imperfect Synchronization", in *2010 IEEE 71st Vehicular Technology Conference,* Taipei, *VTC.,* 2010, pp. 1-4.

[4] X. He, X. Zhang, B. Yang, "The effect of imperfect carrier synchronization on the performance of multi-tone DSSS", in *12th IEEE International Conference on Communication Technology,* Nanjing, *ICCT.,* 2010, pp. 637-643.

[5] H. Naqvi, S. Berber, Z. Salcic, "Performance analysis of collaborative communication with imperfect frequency synchronization and AWGN in wireless sensor networks", *Communication and Networking,* CCIS., pp. 114-121, 2009.

[6] H. Naqvi, S. Berber, Z. Salcic, "Performance analysis of collaborative communication in the presence of phase errors and AWGN in wireless sensor networks", in *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, Leipzig, *IWCMC.*, 2009, pp. 394-398.

[7] P. Yang, Z. Tan, A. Wiesel, A. Nehorai, "Power system state estimation using PMUs with imperfect synchronization", *IEEE Transactions on power Systems*, vol. 28, no. 4, pp. 4162-4172. 2013.

[8] R. Mislovaty, E. Klein, I. Kanter and W. Kinzel, "Security of neural cryptography", in *11th IEEE International Conference on Electronics, Circuits and Systems,* Tel Aviv, *ICECS.*, 2004, pp. 219-221.

[9] A.B. Salberg, A. Hanssen, "Secure digital communications by means of stochastic process shift keying", in Proc. Int. Conf. Signals, Systems, and Computers, CA. USA, *Cat. No.CH37020.*, 1999, pp. 1523–1527.

[10] M.E. Cek, F.A Savaci, "Stable non-Gaussian noise parameter modulation in digital communication", IET Electronics Letters, vol. 45, no. 24, pp. 1256–1257, 2009.

[11] M. E. Cek, "Covert communication using skewed α-stable distributions", IET *Elec Let*, vol. 51, no. 1, pp. 116-118, 2015

[12] Z. Xu, J. Yuan, K. Wang, L. Meng, J. Hua, "A Novel Structure for Covert Communication Based on Alpha Stable Distribution", Inform. Technol. J., vol. 13, no. 9, pp. 1673-1677, 2014.

[13] M.E. Cek, "M-ary alpha-stable noise modulation in spread-spectrum communication", Fluctuation and Noise Letters, vol. 14, no. 3, 1550022, 2015.

[14] Z.J. Xu, K. Wang, Y. Gong, W.D. Lu, J.Y. Hua, "Structure and performance analysis of an SαS-based digital modulation system", *IET Comm*, vol. 10, no. 11, pp. 1329-1339, 2016.

[15] Z. Xu, Y. Gong, K. Wang, W. Lu, J. Hua, "A Covert Digital Communication System Based on Joint Normal Distribution", *IET Communications*, vol. 11, no. 8, pp. 1282-1290, 2017.

[16] A. Ahmed, F.A Savaci, "Random Communication System Based on Skewed Alpha-Stable Levy Noise Shift Keying", Fluctuation and Noise Letters, vol. 16, no. 3, 1750024, 2017.

[17] G. Samorodnitsky, M.S. Taqqu, "Stable non-gaussian random processes", Chapman & Hall/CRC, New York, 1994.

[18] A. Janicki, A. Weron, "Simulation and chaotic behavior of a-stable stochastic processes", Chapman & Hall/CRC, New York, 1994.