DOI:10.25092/baunfbed.680778 **J. BAUN Inst. Sci. Technol., 22(1), 269-280, (2020)**

Random number generator based on RF spectrum sensing: energy detector and spectral correlation function approach

Ali Rıza EKTİ[*]

Balıkesir University Faculty of Engineering, Department of Electrical and Electronics Engineering, Cagis Campus, Balikesir.

Geliş Tarihi (Received Date): 07.08.2019
Kabul Tarihi (Accepted Date): 19.12.2019

Abstract

Wireless communication is open and more vulnerable against to authorized and unauthorized users due to the broadcasting nature of wireless radio propagation in contrast to wired networks where two devices connected to each other physically through cables. Thus, assuring a secure wireless radio communication is an important and mandatory task for the 5G and beyond wireless networks. In order to prevent the manipulation and to ensure the privacy of the information, secure cryptographic algorithms are necessary. The performance of the cryptographic algorithms heavily relies on the generation of random keys which are created from the seeds and these seeds must be random. By utilization of the random nature of the wireless spectrum, secure random keys can be produced. Therefore, in this study, spectrum sensing based random number generator (RNG) is proposed in order to detect the unknown received signal and extract the noise part of the signal by simply adopting the second order statistics of the cyclostationary process, spectral correlation function and the energy detector approaches. However, utilization of probability mass function output statistics is also introduced to distinguish the noise and unknown signal. A measurement setup is developed also considering line of sight conditions. Obtained noise statistics are used to generate the random bit streams and the results are fed into the NIST 800-22 test suite to show how well the performance of the spectrum sensing based random number generator. High quality random numbers are obtained which implies that spectrum sensing based RNG can provide secure data transfer directly without any other physical device.

Keywords: *Spectrum sensing, random number generator, cyclostationary, spectral correlation function, energy detector.*

[*] Ali Rıza EKTİ, arekti@balikesir.edu.tr, http://orcid.org/0000-0003-0368-0374

RF spektrum algılamasına dayalı rastgele sayı üreticisi: enerji dedektörü ve spektral korelasyon fonksiyonu yaklaşımı

Öz

Kablosuz iletişim, iki cihazın fiziksel olarak kablolarla birbirine bağlandığı kablolu ağların aksine, kablosuz radyo yayılımının yayın niteliği nedeniyle, yetkili ve yetkisiz kullanıcılara karşı daha açık ve daha savunmasızdır. Bu nedenle, güvenli bir kablosuz radyo iletişimini sağlamak, 5G ve ötesindeki kablosuz ağlar için önemli ve zorunlu bir görevdir. Manipülasyonu önlemek ve bilgilerin gizliliğini sağlamak için güvenli şifreleme algoritmaları gereklidir. Şifreleme algoritmalarının performansı büyük ölçüde rastgele 0 veya 1 ikili sayı bitlerinden oluşturulan rastgele anahtarların oluşturulmasına dayanır ve bu bitler rastgele olmalıdır. Kablosuz spektrumun rastgele doğası kullanılarak, güvenli rastgele anahtarlar üretilebilir. Bu nedenle, bu çalışmada, bilinmeyen alınan sinyalin tespit edilmesi ve sinyalin gürültü kısmının ayrıştırılması için sadece dönemli-durağan işleminin ikinci dereceden istatistiklerinden olan spektral korelasyon fonksiyonunu ve temel enerji detektörü kullanılmaktadır. Bununla birlikte, gürültü ve bilinmeyen sinyalleri ayırt etmek için olasılık kütle işlevi çıktı istatistiklerinin kullanılması da tanıtılmıştır. Görüş hattı koşulları da dikkate alınarak bir ölçüm kurulumu geliştirilmiştir. Elde edilen gürültü istatistikleri, rastgele 0 veya 1 ikili sayı bitlerini üretmek için kullanılır. Ayrıca önerilen spektrum algılama tabanlı rastgele sayı üretecinin performansının ne kadar iyi olduğunu göstermek için NIST 800-22 test yazılımı kullanılmıştır. Spektrum algılamalı RNG'nin başka herhangi bir fiziksel cihaz olmadan doğrudan güvenli veri aktarımı sağlayabildiğini gösteren yüksek kalitede rasgele sayılar elde edilmiştir.

Anahtar kelimeler: *Spektrum algılama, rastgele sayı üreticisi, dönemli-durağan, spektral korelasyon fonksiyonu, enerji detektörü.*

1. Introduction

Due to the ever-–increasing demands and applications in wireless communication systems, there is a huge amount of increase in over-the-air signaling. Especially in mobile communication systems, radio frequency (RF) spectrum is getting crowded. The limited capacity in available RF spectrum, led the researchers to find better options to utilize the RF spectrum. One prominent example of is to integrate different wireless technologies and adapt the heterogeneous nature of wireless traffic by utilizing heterogeneous wireless networks to increase network capacity, coverage, data rate and so on [1,2]. However, one should note that all the aforementioned advancement can only be possible with by providing secure communication protocols. Therefore, providing privacy and security for the wireless data transmission is one of the biggest challenging task in next generation wireless networks (NGWNs) to achieve due to the heterogeneous and broadcasting nature of the wireless transmission, where the signals can be captured and recorded by malicious devices. This results not only in accessing their data illegitimately by eavesdroppers, but also in using this data to launch attacks such as identity–based attacks [3]. A great example of such attacks can be observed with Industry 4.0 revolution where many 3G/4G/5G enabled internet of things (IoT) devices are utilized in manufacturing sector in where $178 billion is invested in 2016. Almost one–third of all cyber attacks were launched against manufacturing sector due to the fact that even the most sophisticated manufacturing plants were not designed entirely resilient against cyber–security crimes. Furthermore, recent studies have pointed out a large number of security issues that might be caused by informed cyber–physical attacks on the communication networks ranging from service interruptions, blackouts, and economic losses to life threats. Despite intensive research efforts to defend the communications against cyber–physical attacks, there is no general solution to cope effectively with such threats. Currently, we are witnessing a huge deployment of devices, sensors, actuators, computing machines and robots that are connected to the Internet under the umbrella of a massive machine-to-machine (M2M) and IoT–ecosystem. These IoT devices and their users are expected to interact with each other over wireless links and operate in a self–organized manner to deliver intelligent services and solutions to the challenges faced by the upcoming deployment of smart cities, smart homes, and smart grids.

Based on the aforementioned reasons, providing a secure communication for mobile users and IoT devices while identifying and selecting the most appropriate network or transmission scheme is mandatory for NGWNs. Thus, all mobile devices and IoT devices are expected to generate random bit–streams through RNGs in order to prevent the data theft in the cyber–security domain and ensure the cryptography [4–7]. Hence, it is a must to use an appropriate hand–shaking protocol by using random keys for the encryption and decryption of transferring data. There are two types of RNGs named as pseudo random number generator (PRNG) which generates random numbers through software and true random number generator (TRNG) obtains the random numbers using the hardware which is hard to predict. Thus, obtaining random numbers through TRNGs is a safe process [8]. Therefore, this paper proposes an approach to obtain the RNG by utilizing the random nature of the wireless RF spectrum and sensing the noise part of the signal by simply applying cyclostationary based methods and simple energy detector method.

Smart communication devices are expected to sense, identify and detect the RF spectrum which are deployed in many commercial and tactical fields [9]. The most well–known spectrum sensing methods are cooperative sensing, feature extraction and energy detection [10–13] to select the most appropriate frequency band to initiate the communication between two devices. In literature, there are many studies focusing on experimental validation of the spectrum sensing [13,14]. Since energy detection based spectrum sensing method does not need any pre–information about received signal and computationally complex algorithms, energy detector becomes the designated optimum detector in the absence of information regarding received signal [13–15]. However, one should note that in order to achieve good results with energy detector, signal–to–noise ratio (SNR) value should be high. Especially, for the signals buried under noise, energy detector approach will not provide any accurate information regarding spectrum occupancy. With the introduction of the cyclostationary to the signal identification, the features extracted from cyclostationary process enable researchers to provide more robust signal identification methods [9,16] especially in the area of modulation identification and wireless technology identification. In [17], it is shown that cyclostationary approach can be used to identify PSK, FSK and QAM modulated signals. [18] show that second order cyclostationary features can be used to identify

GSM and LTE signals by utilizing the cyclic features of the wireless air interface technology.

With that being said, the usage of the cyclostationary features such as spectral correlation function (SCF) and energy detector are not investigated for the purpose of the RNG in the literature. Therefore, in this study, it is shown that spectral correlation function output can be used as a spectrum sensing method along with the traditional energy detector approach. Thus, spectral correlation function and energy detector methods are used to distinguish the received signal and noise part of the received signal for sufficient number of samples. In addition to this, probability mass function (PMF) statistics along with energy detector algorithm is utilized to detect the binary phase shift keying (BPSK) modulated signal. We show that the performance of the energy detection changes drastically with respect to the number of samples selected at the receiver side. Furthermore, noise statistics are obtained to generate the random numbers and the results are fed into the National Institute of Standards and Technology (NIST) 800-22 test suite to show how well the performance of the spectrum sensing based RNG [19].

1.1. Organization of the paper

The rest of the paper is organized as follows: In Section 2, statement of the problem and signal model are provided. In Section 3, spectral correlation function and energy detection are given. In Section 4, the experimental setup, data collection and data processing are presented. This is followed by experimental results in Section 5. Conclusions are drawn in Section 6.

2. Signal model

In this study, the SCF output of the second–order cyclostationary statistics and energy detector approaches are used to detect the presence of the noise and then utilized to extract noise statistics to provide random seeds to generate a RNG for BPSK signal under the absence of the knowledge of the over-the-air signal.

A general expression for unknown M–PSK modulated signal can be given as [20]:

$$\varphi_{PSK}(t) = \mathrm{Re}\left[k(t)e^{j2\pi(u-1)/M}e^{j2\pi f_c t}\right];\ u = 1,\ldots,M \tag{1}$$

where the carrier frequency and the signal pulse are represented as f_c and $k(t)$, respectively. The baseband received complex envelope of the received signal, r(t), which is composed of unknown transmitted signal, $\varphi_{PSK}(t)$, the complex additive white Gaussian noise (AWGN), n(t), with $\mathbb{C}N\left(0,\sigma_N^2\right)$, and the channel components, h(t) can be shown as:

$$r(t) = h(t)\varphi(t) + n(t) = e^{j2\pi\rho t}\sum_{i=1}^{L}\varphi(t-\tau_i)h_i(t) + n(t) \tag{2}$$

where number of taps, channel effects, tap delays and frequency offset are denoted as L, $h(t)=\sum_{i=1}^{L} h_i(t)\delta(t-\tau_i), \tau_i$ and ρ, respectively. Furthermore, $n(t)=n_I(t)+jn_Q(t)$ where $n_I(t)$ and $jn_Q(t)$ are $\mathbb{C}N\left(0,\sigma_N^2/2\right)$.

3. Spectrum sensing methods

3.1. Spectral correlation function

In this study, we utilize the second–order cyclostationary of signals by taking the non–linear transformation as [16]:

$$\upsilon_\tau(t)=\mathbb{E}\left\{r(t+\tau/2)r^*(t-\tau/2)\right\}, \tag{3}$$

where $\upsilon_\tau(t)$ is the auto–correlation of r(t) and due to the periodicity of the auto–correlation function the Fourier series coefficients can be shown as [21]

$$\Re_r^\alpha(\tau)=\frac{1}{T_0}\int_{-T_0/2}^{T_0/2} u_\tau(t)e^{(-j2\pi\alpha t)}dt \tag{4}$$

$\Re_r^\alpha(\tau)$ denotes the cyclic auto–correlation function and α is the cyclic frequency. One should know that the frequency domain analysis of the r(t) can provide some unique features. After some mathematical manipulations and the help of the cyclic Wiener relation [16], SCF of the r(t) is given as

$$U_r^\alpha(f)=\int_{-T/2}^{T/2}\Re_r^\alpha(\tau)e^{(-j2\pi f\tau)}d\tau \tag{5}$$

Since SCF calculation is computationally cumbersome, we utilize the fast Fourier Transform (FFT) accumulation method (FAM) to reduce the complexity [17]:

$$U_{r_T}^{\alpha_i+q\Delta\alpha}(nL,f_j)=\sum_k R_T(kL,f_m)R_T^*(kL,f_l)j_c(n-k)e^{(-j2\pi kq)/P} \tag{6}$$

where $R_T(n,f)$ is complex–valued demodulates which is the N`-point FFT of r(n) passed through a Hamming window and can be computed as

$$R_T(n,f)=\sum_{k=-N'/2}^{N'/2} b(k)r(n-k)e^{-i2\pi f(n-k)T_s} \tag{7}$$

3.2. Energy Detection and Decision Statistics

Traditional energy detector captures r(t) and calculates the associated energy of the r(t) over a specified bandwidth and duration. The obtained energy detector output value is compared with a selected threshold after averaging out some parts of FFT to decide whether a signal is presented or not. One should note that the selection of the threshold value relies heavily on the noise floor value. Another important aspect in regards to determining the threshold value is the type of signal detection. For instance, increasing the FFT size for narrow band signals will provide better detection performances. Additionally, longer duration results in higher SNR levels. the decision value for the energy detector output, Decision ed[n] can be given as

$$Decision\ \mathrm{e}_d\left[n\right]=\sum_{i=0}^{N-1}\left|r[i]\right|^2 \underset{>}{\overset{<}{}} \gamma \tag{8}$$

where N is the number of samples, γ stands for the selected threshold value to decide whether signal presents or not, r[.] stands for the discrete received signal. It is expected that (4) generates a non–central distribution when signal presents. However, in the presence of AWGN only channel, the distribution becomes a central distribution for H_0. The degree of freedom equals to number of samples, N. Therefore, from the perspective of the central limit theorem (CLT), one should know that the decision statistics are asymptotically normally distributed with a fixed mean and variance when N is sufficiently large. Due to the random selection of the observation period and random nature of where the signal presents, one can apply PMF as a statistical test in order to obtain the values for the signal identification. Therefore, PMF statistics are used to support outputs instead of utilizing probability of detection and probability of false alarm statistics. PMF of the energy detector output statistics to obtain weighting factors, w, to determine signal presence can be calculated as

$$w=\frac{Decision\ \mathrm{e}_d\left[n\right]}{\sum Decision\ \mathrm{e}_d\left[n\right]} \tag{9}$$

3.3. Binary Hypothesis Test

Depending on the idle or busy state of the mobile propagation channel of RF spectrum with the presence of the transmitted signal, the signal detection by utilizing SCF and energy detector can be shown as a binary hypothesis test

$$r(t)=\begin{Bmatrix} h(t)\varphi(t)+n(t), & \mathrm{H}_1 \\ n(t), & \mathrm{H}_0 \end{Bmatrix} \tag{10}$$

H_0 and H_1 are the hypotheses respect to presence of noise only and the unknown signal, respectively. Therefore, the problem statement can be stated as identification of the presence of the unknown signal $\varphi(t)$ and n(t).

4. Measurement setup and data processing

We develop a measurement setup in the Wireless Research Laboratory as seen in Figure 2(a) and illustration of the measurement setup is also shown in Figure 2(b).

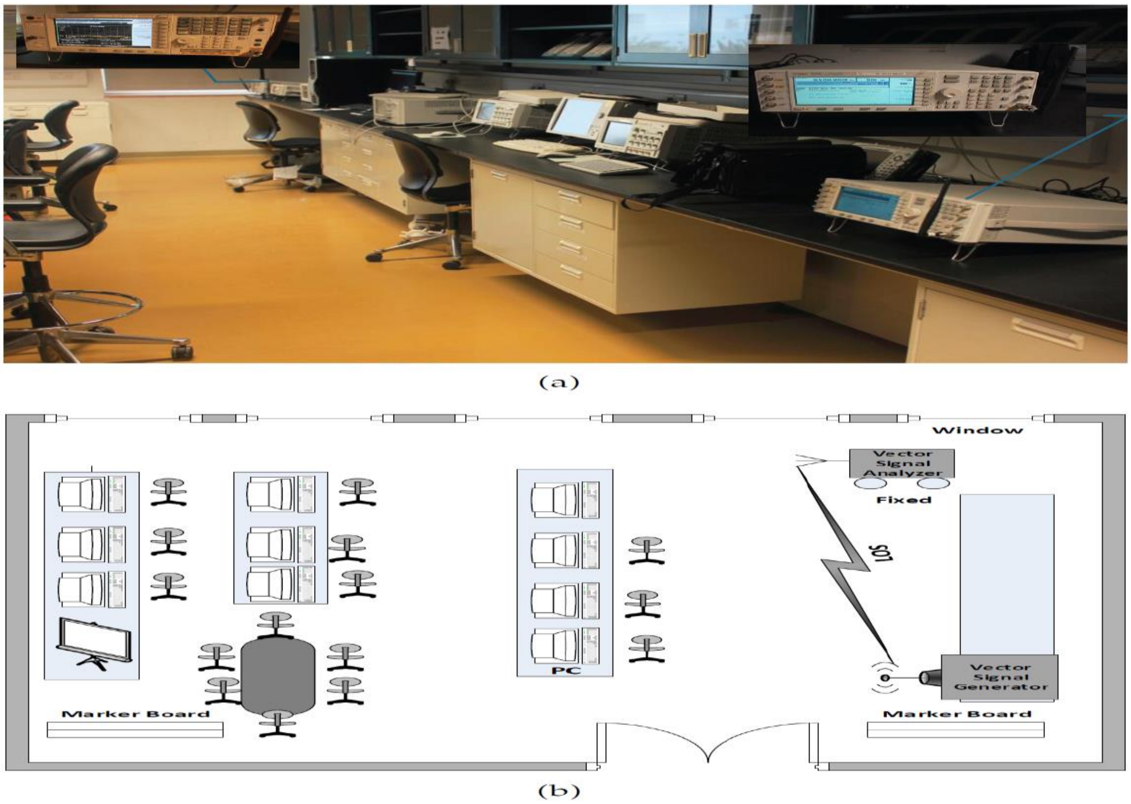


Figure 2. (a) Actual picture of the measurement setup, (b) Illustration of the measurement setup.

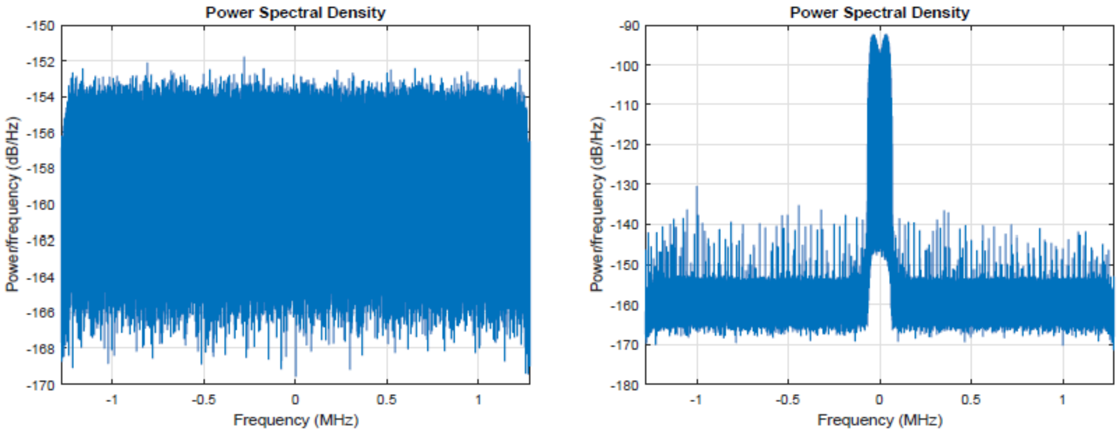
4.1. Measurement methodology and setup

Transmitted signalwith digital BPSKmodulation is generated and transmitted by using an Agilent vector signal generator (VSG) E4438C from a fixed location as shown in Figure 2. The parameters used for signal generation is shown in Table 1. Agilent PSA Series vector signal analyzer (VSA) E4440A is utilized to capture the transmitted signal. in–phase/quadrature (I/Q) samples captured by VSA E4440A transferred into laptop computer and all the analyses are done on MATLAB R2015b software runs.

Table 1. Parameters used to generate the transmitted signal.

Standard	Center Frequency	Symbol Rate	Bandwidth	Power	Alpha Factor
NADC	915Mhz	100kS/s	2Mhz	0dBm	0.35

The noise part of the signal and the actual signal can be seen in Figure 3.



(a) Received signal, $r(t)$, H_0 case

(b) Received signal, $r(t)$, H_1 case

Figure 3. Power spectral density of H_0 and H_1 cases.

4.2. Data processing

For H_0 case, VSG is turned off. Then, we use VSA to capture the ambient thermal noise and we ensure that there is no unwanted signal present. Then, for H_1 case, by utilizing the parameters shown in TABLE I, BPSK signal is generated by VSG. VSA is set to capture the transmitted signal and in order to show the spectral difference between H_0 and H_1case, the power spectral densitys (PSDs) of the noise signal and the r(t) are plotted by using a MATLAB script in Figure 3. Furthermore, MATLAB is used to obtain to provide the PMF statistics along with energy detector outputs for Equation 10.

Furthermore, MATLAB is used to obtain statistics of these I/Q samples by utilizing the SCF based and energy detector based sensing methods. Moreover, average dB/Hz values fromsignal statistics are calculated. An example scenario is shown for 200 samples of the captured data in Figure 4. Then, the average is calculated for every one thousand data points. If the average number is greater than the mean value, "1" is selected, if not, "0" is chosen. A total of 12.5 million binary random bits are generated with this process.

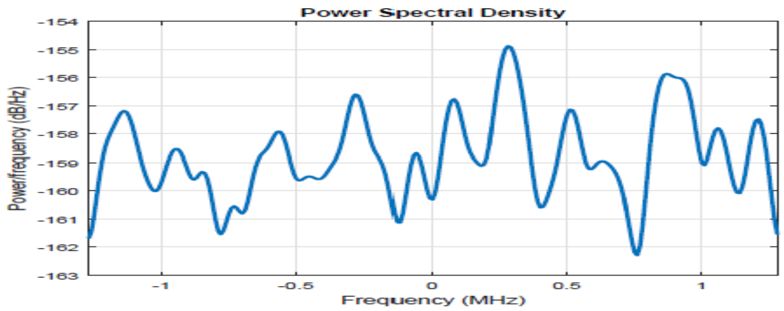
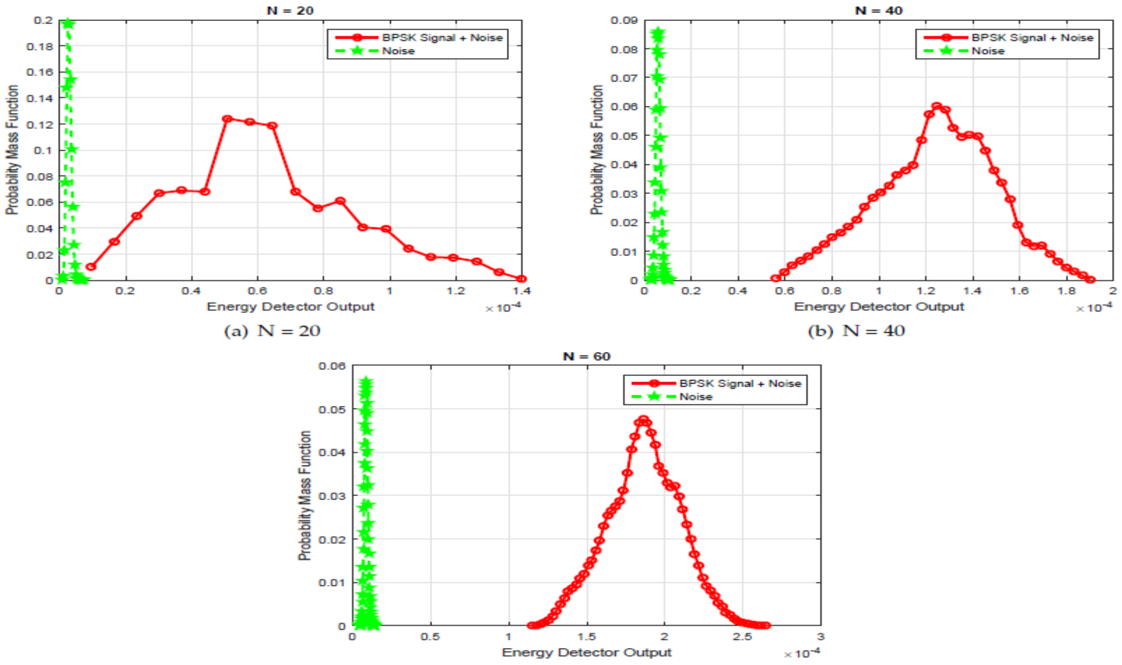


Figure 4. A sample observation of 200 samples of the captured received signal data.

5. Experimental results

Different levels of degrees of freedom is acquired by selecting different number of samples N for Equation 10. One should note that time duration for the captured signal is set to 5 seconds to have adequate amount of statistics in regards to PMF and energy detector statistics. As expected, with the help of CLT, increase in the number of samples resulted in better identification performance as shown in Figure 5. Here, we select number of samples as 20; 40; 60. This way, we can distinguish the noise part of the signal from the actual signal as seen in Figure 3 and utilize the noise part of the signal to generate the random numbers.



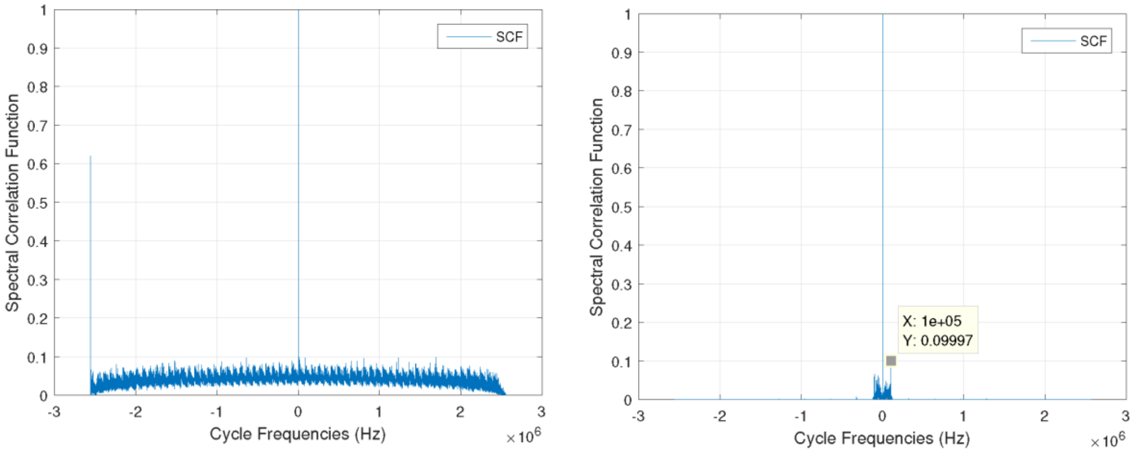
(a) N = 20

(b) N = 40

(c) N = 60

Figure 5. Energy detector output vs PMF output.

In addition to energy detector approach, the SCF of wireless communication signals which are estimated via FAM is depicted in Figure 6. It can be easily seen that SCF of Noise only case and BPSK modulated signal show unique characteristics, they can be employed as feature vectors for a classifier.



(a) Noise only

(b) BPSK and Noise

Figure 6. SCFs estimated for Noise only case and BPSK modulated signal.

The NIST test is applied to random numbers generated and the results are shown in Table 2. One can see that each processed bit stream is random. These results show that properly designed simple energy detector can be used to generate the highly random bit streams and can fulfill the requirements for designing effective RNGs. The minimum average pass rate for all the statistical tests is around 0,98769 for 25 binary sequences except for the random excursions (variant) test which is 0.9 for 10 binary sequences. This implies that that statistical tests provide significant results where the obtained pass rates are above the expected results for both 10–bit and 25–long.

Table 2. NIST–800–22 Test suite results.

NIST Statistical Test	p-value	proportion	result
Block Frequency	0.029796	25/25	PASS
Frequency	0.392456	25/25	PASS
Runs	0.242986	24/25	PASS
Cumulative Sums	0.186566	25/25	PASS
Rank	0.484646	24/25	PASS
Longest Run	0.311542	24/25	PASS
Non Overlapping Template	0.875539	25/25	PASS
FFT	0.392456	25/25	PASS
Overlapping Template	0.141256	25/25	PASS
Universal	0.392456	25/25	PASS
Random Excursions Variant	0.213309	9/10	PASS
Random Excursions	0.739918	10/10	PASS
Linear Complexity	0.311542	24/25	PASS
Serial	0.021262	25/25	PASS

6. Conclusions

We investigate the performance of SCF and energy detector detector spectrum sensing methods to generate random bits from the captured over the air BPSK modulated signal. In this study, SCF and energy detector based noise source detection by utilizing the random nature of the wireless RF spectrum and sensing the noise part of the signal are investigated. It is shown that noise statistics obtained through the aforementioned sensing methods can generate the random bit streams and the results are fed into the NIST 800–22 statistical randomness test suite to show the performance of the proposed approach [19]. Obtained results satisfy the requirements for the NIST 800–22 statistical randomness test. In general, more than one signal is presented in the RF spectrum, therefore, in the future research; we will discuss the performance of the proposed algorithm when there is no priori information about the multiple signals on the RF spectrum.

References

[1] Andrews, J.G., Seven ways that HetNets are a cellular paradigm shift, **IEEE Communications Magazine**, 51, 136–144, (2013).

[2] Bennis, M., Simsek, M., Czylwik, A., Saad, W.; Valentin, S., Debbah, M., When cellular meets WiFi in wireless small cell networks, **IEEE Communications Magazine**, 51, 44–50, (2013).

[3] Ericsson, M.R., **Realizing smart manufacturing through**, IOT, (2018).

[4] Bagini, V., Bucci, M., A design of reliable true random number generator for cryptographic applications. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 204–218, (1999).

[5] Schneier, B., **Applied cryptography: protocols, algorithms, and source code in C**; John Wiley & Sons, (2007).

[6] Hong, S.L., Liu, C., Sensor-based random number generator seeding, **IEEE Access**, 3, 562–568, (2015).

[7] Demir, K., Ergün, S., An analysis of deterministic chaos as an entropy source for random number generators, **Entropy**, 20, 957, (2018).

[8] Lee, K., Lee, S.Y., Seo, C., Yim, K., TRNG (True Random Number Generator) method using visible spectrum for secure communication on 5G network, **IEEE Access**, 6, 12838–12847, (2018).

[9] Dobre, O.A., Signal identification for emerging intelligent radios: Classical problems and new challenges, **IEEE Instrumentation & Measurement Magazine**, 18, 11–18, (2015).

[10] Cabric, D., Tkachenko, A., Brodersen, R., Experimental study of spectrum sensing based on energy detection and network cooperation. Proceedings of the first international workshop on Technology and policy for accessing spectrum. ACM, p. 12, (2006).

[11] Yarkan, S., Halbawi, W., Qaraqe, K.A., An experimental setup for performance evaluation of spectrum sensing via energy detector: indoor environment. Proceedings of the 4th International Conference on Cognitive Radio and Advanced Spectrum Management. ACM, p. 42, (2011).

[12] Yarkan, S., A Generic Measurement Setup for Implementation and Performance Evaluation of Spectrum Sensing Techniques: Indoor Environments, **IEEE Trans. Instr. and Meas.**, 64, 606–614, (2015).

[13] Yucek, T., Arslan, H., A survey of spectrum sensing algorithms for cognitive radio applications, **Communications Surveys & Tutorials, IEEE**, 11, 116–130, (2009).

[14] Pawelczak, P., Nolan, K., Doyle, L., Oh, S.W., Cabric, D,. Cognitive radio: Ten years of experimentation and development, **IEEE Communications Magazine**, 49, 90–100, (2011).

[15] Dillard, R.A., Detectability of Spread–Spectrum Signals, **IEEE Transactions on Aerospace and Electronic Systems**, AES – 15, 526 – 537, (1979).

[16] Gardner,W.A., Exploitation of spectral redundancy in cyclostationary signals, **IEEE Signal Process. Mag**., 8, 14–36, (1991).

[17] Roberts, R.S., Brown, W.A., Loomis, H.H., Computationally efficient algorithms for cyclic spectral analysis, **IEEE Signal Process. Mag.**, 8, 38–49, (1991).

[18] Karami, E., Dobre, O.A., Adnani, N., Identification of GSM and LTE signals using their second-order cyclostationary, **IEEE Intl. Instrum. and Meas. Tech. Conf. (I2MTC). IEEE**, 1108–1112, (2015).

[19] Bassham, L.E., Rukhin, A.L., Soto, J., Nechvatal, J.R., Smid, M.E., Leigh, S.D., Levenson, M., Vangel, M., Heckert, N.A., Banks, D.L., A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications – **NIST. Technical Report**, (2010).

[20] Proakis, J.G., **Digital Communications**; McGraw–Hill, New York, 2001.

[21] Giannakis, G.B., Cyclostationary signal analysis, **Digital Signal Processing Handbook**, 17–1, (1998).