Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 117 (2019) 228-234 EISSN 2392-2192

SHORT COMMUNICATION

Empirical assessment of efficiency of entropy source for random number generators using autocorrelation factor test

Shreenabh Moujesh Agrawal

The Chanda Devi Saraf School, Nagpur, Maharashtra, India

E-mail address: agrawalshreenabh@gmail.com

ABSTRACT

To achieve true randomness of numbers, the entropy source needs to be efficient. The statistical testing of efficiency of entropy source is necessary as it is used in random number generators for cryptography, simulation, statistical sampling, etc. 5000 numbers each were generated in four experimental entropy conditions: Control experiment with white light, Experimental conditions with multicoloured light with light path not disrupted, while light with path disrupted by thermocol balls, multicoloured light with path disrupted by thermocol balls. The numbers thus generated using each entropy condition were tested by Auto Correlation Factor Test to identify optimal experimental condition. The results were displayed in graphical and tabular format. The four graphs depicted the autocorrelations clearly showing that the best results were obtained for the fourth experimental condition 'multicoloured light fan on'. It was found that Autocorrelation factor test is a powerful test for empirical assessment of efficiency of entropy source for random number generation. If the random number generator developed by any individual or organization is tested by Autocorrelation factor test, the efficiency of the entropy source can be pre-established thus preventing post hazards like hacking of random numbers. The security of data is a major concern in all areas such as defense, banking, research, designing and evaluation of examinations, etc.

***Keywords*:** Entropy, randomness, cyber-security, auto correlation factor test

(Received 28 December 2018; Accepted 05 January 2019; Date of Publication 06 January 2019)

1. INTRODUCTION

Continuous appearance of news related to cyber security failures, banking frauds, improper allotment of benefits to the eligible beneficiaries through Government schemes such as RTE (Right to Education), Subsidies to farmers, etc. have always posed a problem which needed a solution. On reading the methods and practices used to combat these issues pertaining to data security, application of Random Numbers seemed to be a probable solution.

To be able to survive cyber-attacks, the random numbers used for cryptographic purpose should be truly random. There should not be a way to decipher them either by forward or backward tracking. There has been a lot of research in this area of random number generation since last few decades. Researchers have come a long way from mathematical sequence numbers based PRNGs (Pseudo Random Number Generators) to quantum random numbers based TRNGs (True Random Number Generators).

Many a times, the failure of the particular system of random number generation came to the fore when huge loss of data was reported. To overcome the difficulty a new kind of generator evolved from scientific community. Most of the requirements were handled using software generated random numbers but due to their security concerns hardware random number generators came into being. They used either physical, chemical or environmental phenomena for generating their output such as photoelectric effect, beam splitter, Avalanche noise, shot noise, reverse biased semiconductor junction, Johnson-Nyquist noise, Zener diodes, electromagnetic interference, shift registers, etc.

This was termed as ‘Entropy Source’. More random the entropy source better the quality of random numbers. The question that came to the fore was: “How to assess the efficiency of this entropy source statistically?” On reading the literature, it was found that the randomness of numbers was assessed generally by Kolmogorov Smirnov Test for Uniform distribution and Runs Test for randomness of numbers. But the researchers in this area also commented that these tests were not sufficient to assess the efficiency of the entropy source. Hence a need for identifying a more powerful test was realized.

2. BACKGROUND RESEARCH

2. 1. Problems with existing random number generators

There are several attacks possible on Pseudo Random Number generators such as direct cryptanylitic attack, input based attack and state compromise extension attack. Subverted bits can be generated which may pass without being detected. As they are based on algorithms, they can be easily predicted. In Hardware generators, problems like human interaction, environmental issues, computer source and quantum events increase the cost and decrease the speed.

2. 2. Application of Random Numbers

Areas in which random numbers are used include technical applications in Physics, Engineering, Cryptography, Simulation, Gambling, Gaming etc. The application of random numbers is seen in medical research studies including detection of diabetes, alzhiemer's, etc.

2. 3. Failure of Random Number Generators

Many instances of banking frauds, suicides due to financial losses, data losses, security breach find mention in news articles. These failures are due to the weak entropy source which can easily be hacked.

3. RESEARCH METHODOLOGY

3. 1. Hypothesis

Auto correlation factor test gives good assessment of efficiency of entropy source for random number generation.

3. 2. Experimental Design

A cubical box of softboard with three white LEDs at the bottom, a fan on one side and Arduino board fixed at the top was made to act as the experimental setup. The LEDs were lighted such that the LDRs would get the signal which they would transfer to the Arduino board (pre coded/programmed) which would finally generate the random numbers. These random numbers would be displayed on the serial monitor connected to the setup. This was treated as the **control experimental set up** named white light fan off.

In the second condition, thermocol balls were placed inside the box and the fan was put on thus creating air turbulence. The balls disrupted the path of light from the LEDs to the LDRs. This condition was named ‘white light fan on’.

In the third and fourth experimental conditions, the three white light emitting diodes fashioned in a linear manner were replaced by one white and three multicoloured leds and fashioned in a triangular position. The sensors were also rearranged in a triangular manner. After changing the positions of the leds and sensors, the readings were taken first by keeping the fan off and then by keeping the fan on. These conditions were named ‘multicoloured light fan off’ and ‘multicolored light fan on’.

5000 bers for every experimental condition were recorded.

4. STATISTICAL ANALYSIS

4. 1. Autocorrelation values: Autocorrelation factor test

The numbers generated using the four experimental entropy conditions were tested using Autocorrelation factor test.

Table 1. Autocorrelations for four experimental entropy conditions

Lag	whiteledfanoff	whiteledfanon	multiledfanoff	multiledfanon
1	0.077	0.000	-0.018	-0.014
2	0.038	0.007	0.003	0.016
3	0.000	-0.012	0.004	0.010

4	-0.008	-0.004	-0.003	0.003
5	0.000	0.009	-0.015	0.008
6	-0.016	0.023	-0.037	0.005
7	0.021	-0.010	-0.021	-0.012
8	-0.001	-0.017	0.003	0.016
9	0.081	0.031	-0.021	0.011
10	0.139	-0.007	0.010	-0.015
11	0.041	0.044	-0.002	0.018
12	0.042	-0.018	0.006	0.001
13	-0.007	0.010	0.013	-0.009
14	0.005	0.017	0.006	-0.006
15	-0.005	-0.005	0.012	0.008
16	-0.009	-0.008	0.009	-0.014

4. 2. Autocorrelation Factor graphs for experimental conditions

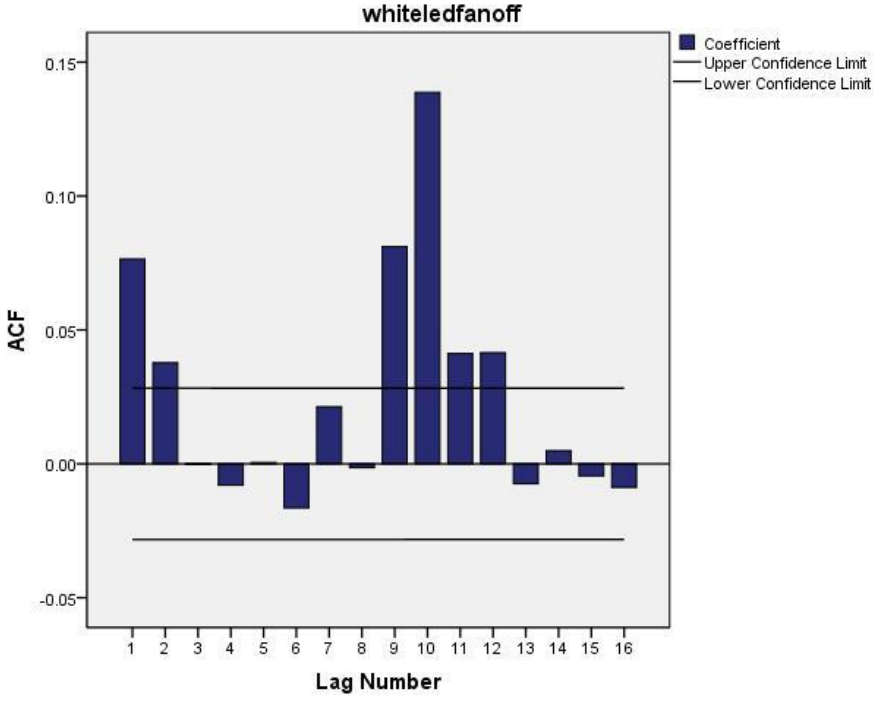

Figure 1. Control experimental set up with White light fan off position

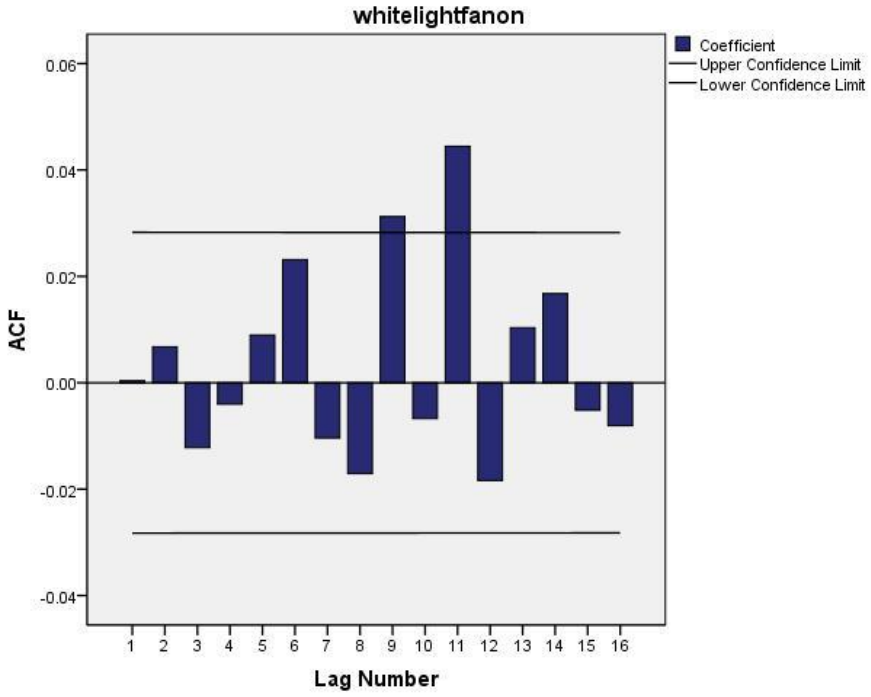

Figure 2. Experimental set up with White light fan on position

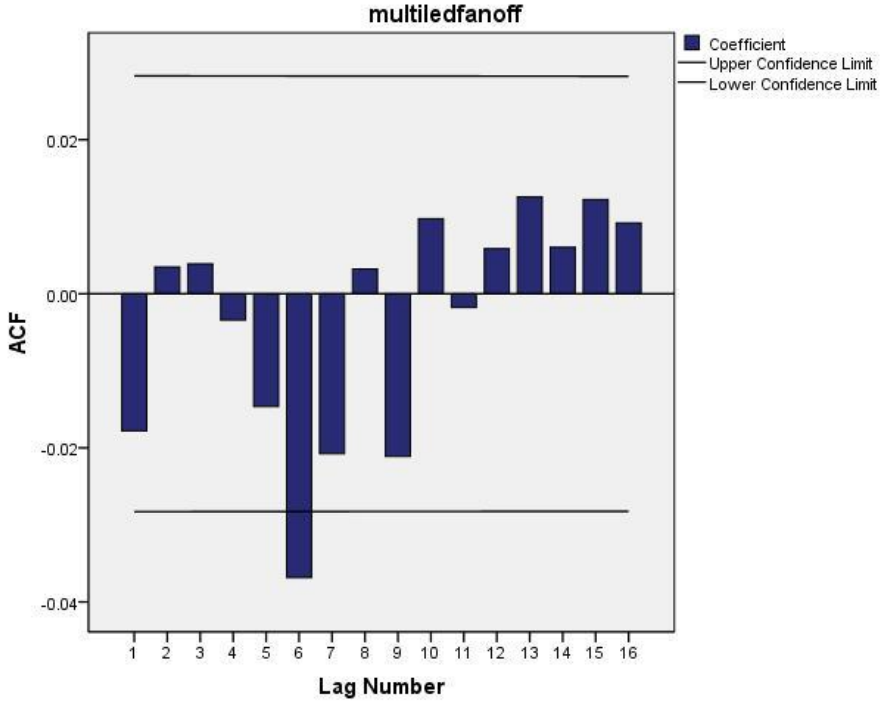

Figure 3. Experimental set up with Muticoloured light fan off position

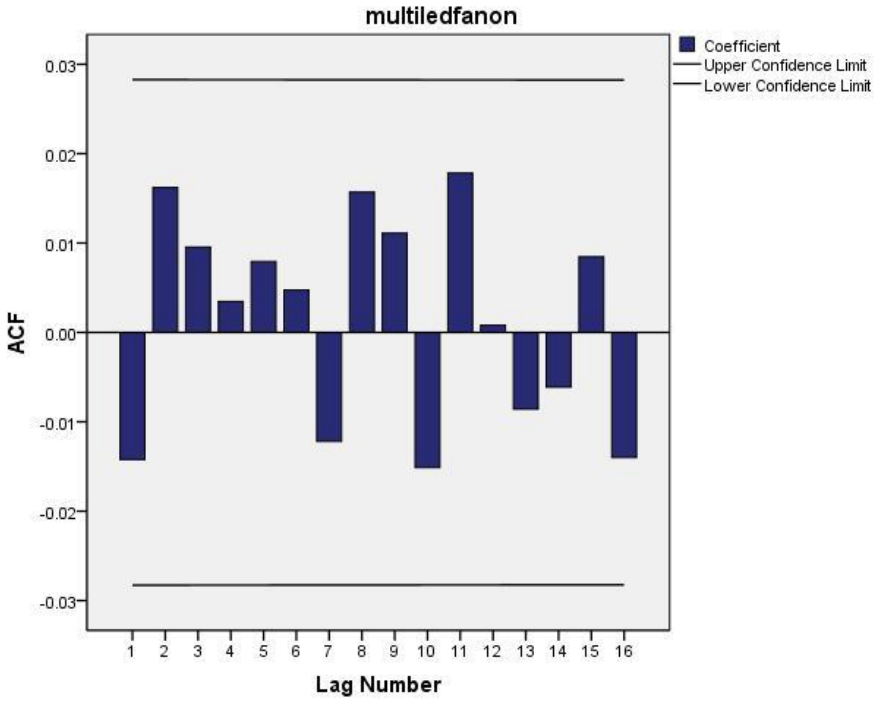

Figure 4. Experimental set up with Muticoloured light fan on position

4. 3. Interpretation

On observing the above graphs (1 to 4) it was found that Graph 4 depicted the best results as the ACF values lied between the UCL and LCL (upper and lower confidence limits) whereas all the other three graphs showed otherwise. Hence, Multi coloured light with fan on position set up was found to be the optimal set up.

5. CONCLUSIONS

The analysis shows that Autocorrelation factor test gives good assessment of entropy source for generating random numbers. If the random number generator developed by any individual or organization is tested by Autocorrelation factor test, the efficiency of the entropy source can be pre-established thus preventing post hazards like hacking of random numbers. The security of data is a major concern in all areas such as defence, banking, research, designing and evaluation of examinations, etc.

Acknowledgement

- Nisha Saraf and Kenneth Mendonca, The Chanda Devi Saraf School, Nagpur, India
- Kartik Kinge, IIIT Nagpur, Co-Founder and Technical Lead, AR Vidhya

Biography

Shreenabh is an innovator and researcher presently studying in Class X of the Chanda Devi Saraf School, Nagpur, Maharashtra, India. At a young age of 15 years, Shreenabh has authored two books and published more than 100 scientific articles in newspapers and magazines. His research includes vital subjects like cryptography, agriculture, sustainable tourism, voice disorder in teachers and scientific temper. His patent on triple lock bore whole lid to save lives of children falling in bore holes has been published. He has to his credit more than 100 national and international certificates (Japan, UK, Korea, Australia and USA). He has won accolades from world renowned Scientists and Diplomats.

References

[1] Bernstein G M, Lieberman M A, Secure random number generation using chaotic circuits, *IEEE Transactions on Circuits and Systems* 37 (1990) 1157-1164

[2] Fishman G S, Moore L R, A Statistical Evaluation of Multiplicative Congruential Random Number Generators with Modulus 2^{31}. *Journal of the American Statistical Association*, 77: 377 (1982) 129-136

[3] MacLaren M D, Marsaglia G., Uniform Random Number Generators, *Journal of the ACM*, 12, (1965) 83-89

[4] Park S K, Miller K W, Random number generators: good ones are hard to find, *Communications of the ACM*, 31 (1988) 1192-1201

[5] Ramsey F L, Characterization of the Partial Autocorrelation Function, *Annals of Statistics*, 2 (1974) 1296-1301

[6] Wichmann B A, Hill I D, Algorithm AS 183: An Efficient and Portable Pseudo-Random Number Generator, *Journal of the Royal Statistical Society. Series C (Applied Statistics)* 31 (1982) 188-190