International Journal of Modern Achievement in Science, Engineering and Technology (IJSET)
ISSN 3023-459X
DOI: 10.63053/ijset.81

A method for generating cryptographic pseudo-random numbers based on 5G radio spectrum for Internet of Things security

Omid NezhadTanavardi[1]

1. Master's Degree in Computer Networks,Islamic Azad University,Tehran,Iran

ARTICLE INFO

Keywords:
Internet of Things, random number generation, 5G, security, entropy, and radio waves..

ABSTRACT

This paper presents a novel approach for generating truly random numbers in 5G wireless communication systems using radio frequency (RF) spectrum. The proposed method utilizes variations in the RF spectrum to create entropy, which is then used to generate truly random numbers. This approach is based on channel state information (CSI) measured at the receiver in 5G systems and leverages the variability of CSI to extract entropy for random number generation. The proposed method has several advantages over traditional random number generators, including the use of a natural source of entropy in 5G wireless communication systems, minimal hardware and computational resource requirements, and a high level of security due to the use of physical characteristics of the wireless channel, which are difficult for attackers to predict or manipulate. Simulation results show that the proposed method produces random numbers with high entropy, passes statistical randomness tests, and performs better than traditional random number generators in terms of energy consumption and computational complexity. This approach has the potential to enhance the security of encryption protocols in 5G networks.

Introduction

The expansion of the Internet of Things has led to an unprecedented increase in connected devices, thus creating the need for secure communication channels. With the development of fifth-generation wireless communication systems (5G), the demand for secure communication channels has become even more critical. The 5G technology provides higher bandwidth, lower latency, and higher data rates, and it is expected to transform the way we interact with the Internet.

However, deploying 5G networks in large, heterogeneous, and distributed environments poses a significant security challenge. To tackle this challenge, secure communication protocols are essential to protect communications between nodes and defend against malicious attacks. One of the critical challenges in 5G security is the generation of secure random numbers. Random Number Generation (RNG) is vital to ensure cryptographic security in various applications, including digital signatures, encryption protocols, password generation, game development, and data transmission. Cryptographic applications require a high-quality random source to produce keys and other secret parameters. Therefore, generating truly random numbers is crucial to ensure the security of these applications. However, in 5G networks, the randomness of generated numbers is unreliable due to low entropy sources that are prone to attacks or failures. The quality of random numbers plays a significant role in the security of cryptographic protocols, including Diffie-Hellman key exchange algorithms (ECDH) and Rijndael encryption algorithms, which are commonly used in 5G networks. Numerous cryptographic protocols have been compromised due to the use of low-quality random numbers. Hence, developing a reliable RNG solution to ensure higher security for communication protocols in 5G networks is vital.

In the world of computing, there are several ways to generate random numbers. Depending on the type of use, different types of generators exist. Random Number Generators (RNGs) comprise a broad category of all these generators. This broad definition of RNG is also known as a Random Bit Generator (RBG), which has been introduced by the National Institute of Standards and Technology (NIST) in the United States. NIST has established a hierarchy of RNGs based on their security level, categorizing them into two types: Non-Deterministic Random Bit Generators (NRBG) and Deterministic Random Bit Generators (DRBG). NRBGs are also referred to as True Random Number Generators (TRNG), while DRBGs are known as Pseudo-Random Number Generators (PRNG). NRBGs are considered the most secure.

Various methods exist for generating random bits, such as hardware-based solutions, software-based solutions, and hybrid solutions. Hardware-based methods rely on physical processes, such as radioactive decay or thermal noise, to generate randomness. These methods have been in use for years and are recognized for their ability to produce random numbers with high entropy. However, they are expensive and require specialized hardware, which gives them less scalability. Software-based approaches rely on mathematical algorithms to produce random bits. These methods are less secure than hardware-based methods, as they may be vulnerable to attacks, but they are more cost-effective and easier to implement. Hybrid solutions combine hardware and software-based approaches to generate random numbers. They typically rely on a hardware-based entropy source that is subsequently used in a software-based PRNG. The hybrid approach provides a good middle ground, offering both high entropy and scalability.

In the field of 5G security, the generation of truly random numbers is essential to ensure the confidentiality, integrity, and availability of communication channels. However, traditional random number generators (RNGs) may not suffice for the requirements of 5G systems, as they may not generate sufficient entropy or may be vulnerable to attacks. Consequently, there is a need for new and more robust RNGs that can provide the necessary level of security.

Given the importance of this issue, numerous studies have been conducted in this field. Alireza Akhti, in 2020, examined "Random Number Generators Based on RF Spectrum Measurement with an Energy Detector Approach and Spectral Correlation Function Approach." In this study, an RNG based on spectrum sensing was introduced to detect unknown received signals and extract the noise component of the signal using second-order statistics of cyclostationary processes, spectral correlation functions, and energy detector approaches. The statistical data obtained for noise was utilized to produce streams of random bits, and the results were submitted to the NIST 22-800 experimental set. High-quality random numbers were obtained, demonstrating that the spectrum-based RNG can facilitate secure data transmission directly without any additional physical devices. Additionally, in another study, Sohail Abbas and colleagues, in 2021, investigated the enhancement of Internet of Things (IoT) security through an RF fingerprint-based device identification system. The proposed technique was tested on a 4G-LTE network for hybrid device recognition within and between manufacturers. Utilizing a cost-effective software-defined radio, the method captures smartphone broadcasts with lower sampling rates. The results indicate that their proposed method provides a classification accuracy of 95.6percent across various signal-to-noise ratio (SNR) levels. Recently, an increasing number of researchers have explored using RF spectrum to generate random numbers. The RF spectrum refers to the frequencies used for wireless communications, and the signal strength and variations in noise can create entropy for producing truly random numbers. Compared to traditional RNGs, RF-based RNGs offer greater entropy, enhanced security, and reduced energy consumption. However, challenges such as calibration and vulnerability to attacks must be addressed for successful implementation.

This study presents a novel method for generating random numbers in 5G wireless communication systems utilising variations in the RF spectrum. This approach creates entropy and generates truly random numbers that potentially surpass the limitations of traditional RNGs. By evaluating the performance of this approach using criteria such as entropy, security, and energy consumption, its effectiveness in providing a more secure and efficient method for generating random numbers in 5G systems can be determined. The feasibility of the proposed methods will be tested using NIST SP 90-800B. The test data were produced through a simulation package in MATLAB.

1. Research Methodology

The methodology employed in this study involves the collection of experimental signals from wireless communication channels, which are utilized to compute the selected frequency band value. Entropy values serve as the seed for generating a sequence of random numbers. Once a spectrogram is produced, the subsequent phase entails extracting entropy from the entropy source. This process involves measuring the unpredictability of the magnitude spectrum, which is employed to generate a sequence of random numbers. These numbers must undergo multiple statistical tests to ensure they possess high quality and are suitable for cryptographic protocols. The proposed algorithm presents a reliable and efficient method for generating random numbers in Internet of Things devices using the available experimental signals within wireless communication systems. This approach can significantly enhance the security of cryptographic protocols by providing high-quality random numbers for the generation of secret keys. Figure 1 illustrates the extraction method of the 5G spectrum, which can be implemented from any 5G Internet of Things device exhibiting noise (for instance, individuals with 5G mobile phones in motion, weather conditions, and other wireless devices operating within the same spectrum) using the 5G toolbox simulated in MATLAB.

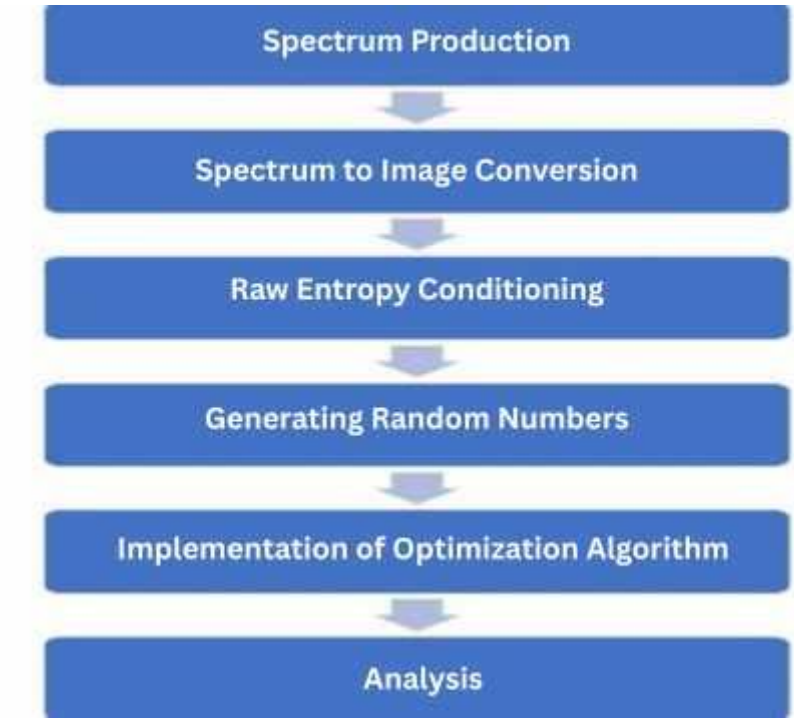

Figure (1): Method of extracting the spectrum of 5G from each 5G Internet of Things device.

The specifications of the utilized system are as follows: 64-bit Windows 10 operating system, Intel(R) Core(TM) i5-7300HQ CPU @ 2.5 GHz, 16 gigabytes of RAM, NVIDIA GeForce GTX 1050 graphics, and storage space of HGST HTS721010A9E630:1T, 7200 RPM.

In summary, it can be stated that in the proposed method, signals from the 5G radio spectrum are generated and subsequently converted into images. These images are predominantly conditioned to enhance randomness. The conditioned images are utilized to produce a random number generator, which is used in optimization employing NSGA2 for optimizing the results of a NIST test set. A brief analysis of the results is conducted using the provided charts and algorithms.

-1-1Spectrum Generation

The dataset used for spectrum generation was developed using the MATLAB 5G toolbox. This dataset comprises frames each with a duration of 40 milliseconds, and each frame was randomly shifted within the frequency domain. It was assumed that 5G signals lie within the specified frequency band, and the network performance was evaluated based on varying random bands. A sampling rate of 44.61 megahertz was deemed adequate for effective 5G processing. In order to generate the corresponding RGB spectrogram images of size 169×369, complex baseband signals were transformed using a Fast Fourier Transform of length 4096. The specifications of the parameter generation for all data are as follows :

5 -G Radio Parameters :

Bandwidth [10, 15, 20, 25, 30, 40, and 50] megahertz, Subcarrier Spacing (SCS): 15 and 30 kilohertz, SSB Period: 20 milliseconds

-Channel Parameters for 5G :

SNR [40 -50 - 100] decibels

Doppler: [0 - 10 - 500] hertz

-Data Generation Parameters :

Number of frames: 2048 integers

Image size: 612 by 14

Number of subframes: 40 milliseconds

Sampling rate 44.61 megahertz

The spectrum data were converted into images using the matplotlib package in Python. The data were split into training and validation datasets, with 2016/32 data points assigned to each. The training data were predominantly utilized for all experiments, as they were foundational for most generated images. To ensure that the resultant images did not contain large white spots, the data were plotted and magnified prior to conversion into images, subsequently being saved in PNG format. The resultant images possessed a size of 169 × 369 pixels. For these images to serve as a source of entropy, they must be loaded into an array from which the selected frame size is used to condition the data for entropy source generation .

The proposed algorithm 5G-SRNG [15] is applied for conditioning the extracted entropy from the spectrogram utilizing the specified frame size and is outlined as follows :

Algorithm 1 Proposed 5G-SRNG [15]

Require: 5G Spectrogram : D ∈ Rmx n, framesize : c,k
1: xstart, ystart ← random(0,m − c), random(0, n − k)
2: xend = min(xstart + c)
3: xend = min(ystart + k)
4: frame ← D[xstart : xend, ystart : yend].f latten()
5: seed ← 0 ▷ Initialize seed with 32-bit float representation of 0
6: for t ∈ frame do
7: seed ← seed ⊕ t ▷ XOR operator
8: seed ← seed ⊕ seed << 13 ▷ Shift-left the previous seed value 13 bits, then perform XOR operator
9: seed ← seed ⊕ seed >> 17 ▷ Right-right the previous seed value 17bits, then perform XOR operator
10: seed ← seed ⊕ seed << 5 ▷ Shift-left the previous seed value 5 bits, then perform XOR operator
11: end for
12: return seed

The proposed 5G-SRNG algorithm can be implemented on Internet of Things devices with minimal hardware requirements. This algorithm utilizes only basic arithmetic and logical operations, which can be effectively executed using either hardware or software. Moreover, this algorithm requires minimal memory, as it only needs to store a single value (i.e., seed) during its execution.

-2-1Generation of Random Numbers

In this article, a total of ten types of Random Number Generators (RNG) and Cryptographically Secure Random Number Generators (CSPRNG) were utilized for the generation of random numbers using a conditional seed. Specifically, we employed PCG64, PCG64XSDM, MT19937, Philox, SFC64, ChaCha, AESCounter, HC128, SPECK128, and ThreeFry .

The algorithm for random number generation is presented in Algorithm 2, ensuring that the generated data complies with the testing requirements. The NumberOfElements and size were selected to meet the minimum necessary requirement of 1,000,000 numbers for universal statistical testing in the NIST test suite. The numbers generated were subjected to testing using the NIST SP 800-22 test suite, with a total of ten distinct PRNG and CSPRNG implementations, thereby assuring a comprehensive evaluation of the randomness of the generated data.

Algorithm 2 Random number generation

Require: Generator and seed
1: Generator ← Generator(SeedSequence(seed)) ▷ Initialize the chosen generator with the seed.
2: size ← 2012
3: arr ← [ ]
4: for i ∈ size do
5: arr.extend(Generator.generate(low, high, numberOfElements))
6: bin_arr ← [ ]
7: for i ∈ arr do
8: bin_arr.append(Binary(String(arr[i])))

9: bin_data ← "".join(bin_arr)
10: return bin_data

1- Results

-1-2Shannon Entropy

Shannon entropy is a measure of uncertainty or randomness associated with a random variable, first introduced in information theory. In this article, Shannon entropy is employed to evaluate the quality of the proposed entropy source. The performance of the entropy source was examined through tests of four distinct random number generators (RNGs), both with and without a seed from the 5G-SRNG. For each RNG, 200 numbers were generated within the range of 0 to 32. Subsequently, the frequency distribution of each number was recorded in tables, and Shannon entropy was calculated based on the ratio of the occurrence of each number to the total count. The maximum value of Shannon entropy in this configuration is log2(32) = 5, which serves as the upper limit for the expected entropy. Experimental results for the four different RNGs are presented in Table 1. It is demonstrated that Shannon entropy with a seed from the proposed method utilizing 5G resembles the results obtained from well-known secure random number generators, such as the Windows Random System.

Table (1): Results obtained from the calculation of Shannon entropy using different loops and grains.

values	and parameters RNG
4/9268322055833277	Numpy random (No seed)
4/8837209490338741	Random Windows System
4/9197439582793259	ChaCha and 5G SRNG seed
4/8494091755251345	PCG64 and 5G SRNG seed

The results presented in Table 1 indicate that the utilization of an entropy source generated from 5G RF is acceptable. The choice of which Random Number Generator (RNG) to use may not be crucial in attaining a higher value. However, the selection of a different RNG is significant for other criteria, such as whether it is intended for cryptographic applications or not. The results pertaining to Shannon entropy and the average results from the NIST test suite possess limited intrinsic value. Nonetheless, both provide a broader foundation for drawing conclusions regarding the validity of using 5G radio spectrum as an entropy source.

-2-2Results of NIST SP 800-90B

Table 2 presents the results of various entropy source tests from NIST SP 800-90B, including IID permutation tests, chi-squared tests, linear complexity tests (LRS), and re-seeding tests. These assessments evaluate the capability of the entropy source to generate truly random and unpredictable data that can be utilized for cryptographic key generation. From the table, it is observed that all tests have been passed, and furthermore, the minimum final entropy is approximately 0.2136.

Table (2): Results of the NIST SP 800-90B Entropy Source Testing

Conditional Entropy	Raw entropy	Test Name
Acceptable	Acceptable	IID Permutation tests
Acceptable	Acceptable	Chi-square tests
Acceptable	Acceptable	LRS test
Acceptable	Acceptable	Restart Test
0/3582	0/2145	Min-Entropy Estimate
0/2136		Conditioning test h_out

It is noteworthy that all tests in Table 2 have been successfully completed, indicating the high quality of the generated data .
Additionally, the table presents the estimated minimum entropy, which reflects the amount of extractable entropy from the data. The process of conditionalizing has enhanced the conditional entropy estimation, which is desirable for cryptographic applications. The raw entropy estimate stands at 0.2145 bits per bit, whereas the conditional entropy estimate is 0.3582 bits per bit .
Moreover, the conditionalization test, h_out, included in the table provides insights into the effectiveness of the conditionalization process. With a value of 0.2136 bits per bit, the conditionalization process has not significantly reduced the entropy of the data .
These results indicate that the entropy source generates high-quality, random, and unpredictable data suitable for cryptographic applications .

-3-2Comparison of Entropy Results

An initial comparison of the results obtained from NIST SP 800-90B concerning the compression of data files using CMIX has been conducted. Table 3 presents the results of both the conditional data set and the raw data set derived from the entropy source. The results are provided using the minimum entropy estimation from both CMIX and NIST SP 800-90B .

Table (3): Comparison of the Minimum Entropy Reported for NIST SP 800-90B against the CMIX Compression Tool

CMIX[15]	SP800-90B	dataset
0/5531	0/3582	conditional
0/2998	0/2145	raw

Based on the data presented in Table 3, it can be observed that the entropy estimate in SP800-90B yields results that are relatively close to those based on compression. In certain forums and online platforms, the results obtained from the entropy estimation of NIST SP 800-90B have been called into question, with assertions that they present excessively conservative outcomes. This discrepancy may also stem from this consideration.

4-2- Execution Time of Experiments

All results related to execution time have been recorded and are presented in this section.
Some experiments were conducted using a version of the code to obtain entropy sources for generating a large quantity of entropy. Executing this on a standard free software package in Google Colab demonstrated that utilizing matplotlib for reading images resulted in approximately 100 It/s, while using cv2 led to 130 It/s.
To generate a dataset for the NIST SP800-90B test set, a minimum of 1,000,000 samples was required. This necessitated an execution time of over two hours to produce all samples using this method. Consequently, experiments were carried out to identify the limitations of the current conditionalization algorithm. These experiments employed twenty distinct images and were conducted in two scenarios: one with images of minimal frame size (1,1) and the other with maximum frame size (369,169). The execution times are presented in the list below:
• Execution time for a test with conditionalization of 20 different images is provided.
• Best case (c, k) = (1, 1): 0 to 0.5 seconds
• Worst case (c, k) = (369, 169): 24 minutes and 12 seconds

3.Conclusion

This study introduces a novel method for generating random numbers in 5G wireless communication systems. It utilizes the radio frequency spectrum as a source of entropy and extracts entropy from the variability of channel state information. The resultant random numbers exhibit

high quality and a significant level of entropy. Simulations conducted using the proposed method in a 5G system model demonstrate superior performance in terms of energy consumption and computational complexity compared to traditional random number generators (RNGs). The proposed method represents a substantial advancement in the field of random number generation and has the potential to resolve the challenges associated with unreliable random number generation in 5G networks. Furthermore, the efficacy of the proposed method can be further validated by comparing its performance with other advanced RNG techniques.

References :

1.Rose, K., S. Eldridge, and L. Chapin, *The internet of things: An overview.* The internet society (ISOC), 2015. **80**(15): p. 1-53.
2.Sfar, A.R., et al., *A roadmap for security challenges in the Internet of Things.* Digital Communications and Networks, 2018. **4**(2): p. 118-137.
3.Chasaki, D. and C. Mansour, *Security challenges in the internet of things.* International Journal of Space-Based and Situated Computing, 2015. **5**(3): p. 141-149.
4.Azrour, M., et al., *Internet of things security: challenges and key issues.* Security and Communication Networks, 2021. **2021**(1): p. 5533843.
5.Crocetti, L., et al., *Design and test of an integrated random number generator with all-digital entropy source.* Entropy, 2022. **24**(2): p. 139.
6.Lu, T., *A survey on risc-v security: Hardware and architecture.* arXiv preprint arXiv:2107.04175, 2021.
7.Celik, A., et al., *A top-down survey on optical wireless communications for the internet of things.* IEEE Communications Surveys & Tutorials, 2022. **25**(1): p. 1-45.
8.Noor, M.A., et al., *5G mobile wireless access and digital channeling with RF over fiber for long-haul 64-QAM communication.* IETE journal of research, 2024. **70**(4): p. 3307-3320.
9.Cameron, T., *Bits to beams–RF technology evolution for 5G mmWave radios.* Analog Devices, Norwood, MA, USA, Tech. Rep, 2019.
10.Zi, R., et al., *Energy efficiency optimization of 5G radio frequency chain systems.* IEEE Journal on Selected Areas in Communications, 2016. **34**(4): p. 758-771.
11.Hussein, A.I., et al. *Design of receiver RF front end for mm-Wave 5G applications*. in *2024 21st Learning and Technology Conference (L&T)*. 2024. IEEE.
12.Ekti, A.R., *Random number generator based on RF spectrum sensing: energy detector and spectral correlation function approach.* Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 2020. **22**(1): p. 269-280.
13.Abbas, S., et al., *Improving security of the Internet of Things via RF fingerprinting based device identification system.* Neural Computing and Applications, 2021. **33**(21): p. 14753-14769.
14.Oyewobi, S.S., K. Djouani, and A.M. Kurien, *Visible light communications for internet of things: Prospects and approaches, challenges, solutions and future directions.* Technologies, 2022. **10**(1): p. 28.
15.Øksendal, O.N., *5G RF Spectrum-based Cryptographic Pseudo Random Number Generation for IoT Security*. 2023, uis.