Bulletin of Electrical Engineering and Informatics
Vol. 13, No. 4, August 2024, pp. 2707~2715
ISSN: 2302-9285, DOI: 10.11591/eei.v13i4.7019

Security-based low-density parity check encoder for 5G communication

Balamurugan Rajangam[1], Manjunathan Alagarsamy[2], Chirakkal Rathish Radhakrishnan[3], Tsehay Admassu Assegie[4], Ayodeji Olalekan Salau[5,8], Andrew Quansah[6], Nur Mohammad Chowdhury[7], Ismatul Jannat Chowdhury[6]

[1]Department of Electronics and Communication Engineering, K. Ramakrishnan College of Engineering, Tamil Nadu, India
[2]Department of Electronics and Communication Engineering, K. Ramakrishnan College of Technology, Tamil Nadu, India
[3]Department of Computer Engineering, New Horizon College of Engineering, Bengaluru, India
[4] School of Electronics Engineering, Kyungpook National University, Daegu, Republic of Korea
[5]Department of Electrical/Electronics and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria
[6]Department of Electrical and Computer Engineering, University of North Carolina at Charlotte, Charlotte, USA
[7]Department of Computer Science, Louisiana Tech University in Ruston, Los Angeles, USA
[8]Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Tamil Nadu, India

Article Info

Article history:

Received Jun 18, 2023
Revised Feb 8, 2024
Accepted Mar 15, 2024

Keywords:

5G
Encoder
Low-density parity check codes
Security
Side-channel attack

ABSTRACT

The fifth generation (5G) of mobile telecommunication standards is intended to offer better performance and efficiency. One of the most significant difficulties in delivering safe data transfer through the transmission channel in the emerging 5G technology is channel-coding security. This research primarily focused on offering information transmission that is secure in the place of novel assaults such as side-channel attacks. In this research, we present a low-density parity check (LDPC) encoder that is constructed using the multiplicative masking method to overcome side-channel attacks, one of the most significant security concerns for the upcoming 5G system. As a result, it offers greater security, reduced complexity, and higher performance. Power, area, and delay can all be calculated using LDPC codes. Comparing multiplicative masking implemented LDPC encoders to ordinary channel coding techniques in terms of security seen that multiplicative masking implemented LDPC encoders offer more security. The program Xilinx ISE 14.7 can synthesize the analysis. The advantage of multiplicative masking is that it offers a promising level of security through the principle of randomization, which is the foundation of the procedure. According to the analysis, the secured transmission of the data by the proposed multiplicative masking implemented LDPC encoder is increased.

Corresponding Author:

Tsehay Admassu Assegie
School of Electronics Engineering, Kyungpook National University
Daegu, Republic of Korea
Email: tsehayadmassu2066@gmail.com

1. INTRODUCTION

The fifth generation (5G) of mobile communication technology is the most recent mobile communication technology used worldwide. Yet, channel-code security is currently one of the most crucial challenges, particularly in light of recent flaws like side-channel assaults. The main purposes of channel coding are to guard against data corruption in the transmission channel and to ensure that the data sent and received are the same error. The major goal of this study is to use the multiplicative masking approach for low-density parity check (LDPC) codes to defend 5G from side-channel assaults. Side-channel assaults are one method for retrieving data during communication processes utilizing side-channel information [1]. The main targets of side-channel assault strategies are time, electromagnetic fields, and power utilization. We proposed "A security-based low-density parity check encoder for 5G" by including a multiplicative masking method into the LDPC encoder architecture. In next-generation wireless communication systems, the LDPC encoder is used to lessen data transmission errors over jerky or noisy communication channels [2], [3]. Additional applications for LDPC codes in 5G include information theory, LDPC as the forward errors correction (FEC) system, its requirement as a part of 802.11ax (Wi-Fi 6), and its use as data channels in 5G new radio (NR). Earlier hardware implementation of LDPC code techniques is performed by using a field-programmable gate array (FPGA) structure, along with an extra outer errors correction, orthogonal frequency division multiplexing (OFDM) systems, 5G NR data channels, flexible hardware architecture for LDPC encoder, FEC system, and (7) triple-layer cell (TLC) (and later) SSDs. The earlier technique has numerous shortcomings, including greater power, space, and delay consumption. Hardware implementation of some functions can be challenging [4].

The perceived high encoding complexity of LDPC codes is one of their main flaws. Lower triangular technique delay constraint was not emphasized in the FPGA implementation of LDPC encoder algorithms. Flexible hardware architecture avoids comparing the ALT and modified ALT methods, which lessens the complexity of LDPC encoding [5], [6]. The difficulty of LDPC codes is dependent on the coding rate; the greater the code rate, the lower the complexity, and vice versa. Because of the benefits they offer, LDPC codes are seen as a technology that has a good chance of being employed in the following generation of wireless communications systems [7]. Using the multiplicative masking method, we demonstrated in this study that LDPC codes are the codes that control mistakes in message transfers over unsafe or noisy communication channels and improve security. The benefits include no-mistake floors and improved security compared to other codes. Moreover, LDPC codes can do error correction more effectively [8]. In addition, it is employed to lessen the delay and area. Part 2 of this essay, which we found to be the most useful, shows how we reviewed the literature. The fundamentals of basic LDPC codes were covered in section 3, along with a list of the system's shortcomings.

For recursive systematic convolutional, or sub-codes of turbo codes, a new parameter estimate approach is put forth. This technique dramatically enhances performance with less computational complexity [9]. A suitable affine encoder employs one-time pad encryption to increase the security of a cipher text, according to a novel security model for Shannon cipher text [10]. By 2028, the industrial internet of things (IIOT) is expected to comprise roughly 10 billion devices. By seamlessly integrating long-range wide area networks (LoRaWAN) with 4G/5G mobile networks, mobile network operators can reuse existing infrastructure and reuse LoRaWANes. To lessen attacks by Wi-Fi signal, the wind talker analyses Wi-Fi traffic to selectively gather channel state information (CSI) only during password-enter vulnerable periods. This allows it to deduce a user's password entry using CSI and keystrokes [11]. Successive cancellation-based (SC-based) decoders that can generate a list of off-line operations increase polar decoders for the foreseeable future decoding speed, but because the list depends on the code rate, they are not rate-flexible. It suggests a rate-flexible, quick, low-complexity, and high-area decoder using SCs. It developed and tested a prototype 5G mm-wave large multiple input multiple output (MIMO) antenna using standard PCB techniques. It works in the 5G spectrum and is quite selective [12].

2. METHOD

The LDPC encoder may be accomplished using several different sorts of algorithms in this section. The circuit that uses those techniques is ineffective because it doesn't offer much energy, assurance of security, or surface area. It also features a long propagation latency and a complex circuit architecture [13], [14]. The LDPC encoder mentioned above is described as follows.

A subset of linear block codes is known as LDPC codes. The best error correction codes now in use are undoubtedly LDPC codes. Linear block codes with a sparse parity-check matrix are known as LDPC codes. LDPC matrix is known as a sparse parity-check matrix [15]. The phrase "low density" describes a property of the parity check matrix where there are relatively few 1 s as opposed to 0 s.

- H: LDPC matrix
- Number of 1 s <<n(n-k).
- n(n-k) → Total entries in the matrix.

Figure 1 shows the general LDPC coding process. The process first includes the block of the input array to be given to the next process which is the LDPC coding process this is where the encoding of the information takes place. Now the encoded data is sent over a transmission line to the destiny after that it is decoded to get the original information then it is processed and gets as an output array [16].

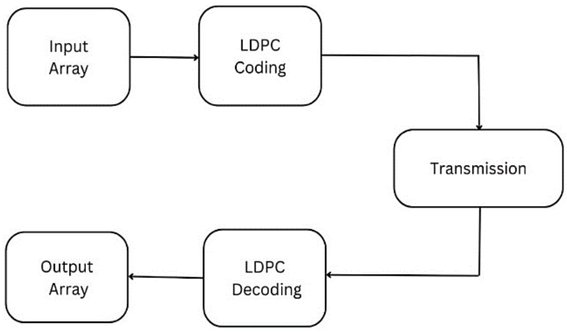

Figure 1. LDPC coding process

3. LOW-DENSITY PARITY CHECK ENCODER

An encoder's primary function is to merge the message bits with a few parity bits to create a code word. The LDPC codes, code length, code rate, and encoding method are a few of the crucial characteristics used in LDPC encoding [17].

$$C = UG \tag{1}$$

In (1) where G is the generating matrix and U is the block of message bits. When H is the parity check matrix, it is possible to tell if a code word is valid by looking at if HCT=0. If the result is not zero, the code word C is invalid, and an error correction procedure should be used. Several LDPC encoding techniques make use of the generating matrix (G) or parity check matrix (H).

During encoding to create a parity symbol, each of the constituent encoders—which are frequently accumulators—is used. Coding symbols are created by combining the original data (S_0, K-1) with parity bits (P). The S bits of each component encoder are ignored. Where U is the block of information bits and G is the generating matrix. Most LDPC encoders' working parts are shown in Figure 2.

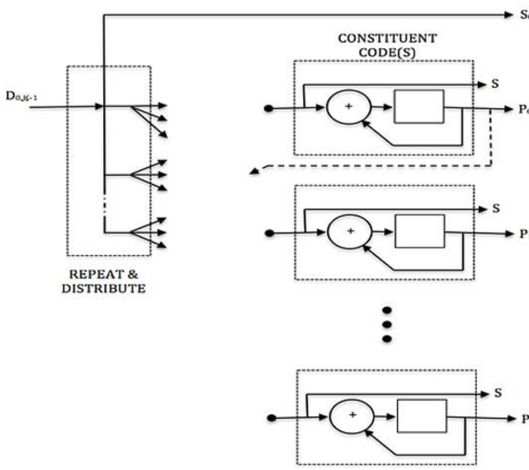

Figure 2. LDPC encoder

3.1. Security-based low-density parity check for 5G

The future of 5G technology is quite bright, but one of the largest challenges is channel-coding security, especially in light of recent vulnerabilities like side-channel attacks. Our suggested design is a highly secure LDBC encoder architecture, which offers a methodical design approach and multiplicative masking method implementation to ensure maximum security in data transmission [18].

3.1.1. Multiplicative masking

One of the primary channel-coding techniques used in 5G is referred to as "LDPC codes". The creation of safe channel coding techniques is one of the most crucial defense strategies for 5G technology's channel coding against side-channel attacks [19]. The multiplicative masking technique is used in the current study for LDPC codes to increase network security for 5G systems. The main contributions of this study are as follows: for LDPC codes, it is advised to multiply in finite fields. A multiplicative masking technique based on a multiplication algorithm is offered to secure LDPC codes [20]. A better LDPC-safe coding method for 5G is built on the multiplicative masking strategy.

Figure 3 shows the multiplicative masking method, where each computation uses a random value. Because each computation's power is unpredictable, it is challenging to extract sensitive information from the LDPC coding. In the finite field GF (2^n), where r can be written as α^k, an element r is generated at random.

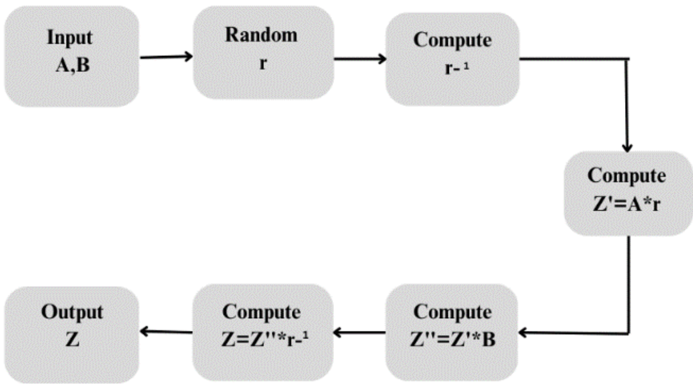

Figure 3. Multiplicative masking method

$$Theinvcerseof\Upsilon iscomputed, i.e, \Upsilon^{-1} = \alpha^{2\wedge n-1-k}$$

$$k'be(i+k)\,mod(\,2^n-1), Z' = A * \Upsilon, i.e., Z' = \alpha^{K'}, isgenerated$$

$$k''be(k'+j)\,mod(\,2^n-1), Z^{''} = Z' * B, i.e., Z'' = \alpha^{K^{''}}, iscomputed$$

$$k'''be = (k''+2^{n-1-k})\,mod(\,2^n-1), Z^{'''} = Z'' * \Upsilon^{-1}, i.e., Z''' = \alpha^{K^{'''}}, iscomputed$$

3.1.2. Multiplication algorithm in a finite field

The finite field GF(p), which has p elements, including 0, 1..., p 1, as an example, has p elements. The singular finite field GF consists of two elements with numbers 0 and 1. The (2) a finite field, and two extensions G, GF(2^n) (2). In contemporary coding, computer theory, combinatory, and other subjects, finite fields are frequently employed. The most frequent finite fields used in LDPC codes are GF(2), GF(p), and GF(2^n). In specific, multi-band LDPC codes benefit greatly from GF(2^n). It is a finite field. GF(2^n) has 2 n elements, i.e., 0, 0, 1, 2..., 2 n2. Multiplication in finite fields is one of LDPC coding's most frequently used procedures. Assuming that A and B are two elements in GF(2^n), where A can be represented as i and B as j, respectively, it is possible to multiply in (2) and (3). Let us assume that when A and B are multiplied, z is the anticipated outcome, then:

$$Z = A * B = \alpha^I * \alpha^J = \alpha^{I+J} \tag{2}$$

Let k=i+j. The multiplication outcome is calculated as follows if k > 2^n-2.

$$Z = \alpha^{K-(2\wedge n-1)} \tag{3}$$

If not, the outcome of the multiplication is $Z = \alpha^K$.

3.1.3. Multiplicative masking algorithm

Channel-coding security is one of the primary communications problems, specifically in light of recent threats like side-channel assaults, even if multi-band LDPC codes can perform error correction more successfully than binary LDPC codes. In these cases, a multiplication algorithm in finite fields-based multiplicative masking technique is suggested [21], [22]. Figure 4 shows the main process of implementation of the multiplicative masking method for LDPC codes. In this process the data undergoes masking and after applying the multiplicative masking method, the secure multiplication, secure addition, and secure Gaussian elimination take place in the designed LDPC encoder [23]. The multiplication of A and B can be done as follows assuming that A and B are two elements in GF(2^n), where A can be written as i and B can be expressed as j.

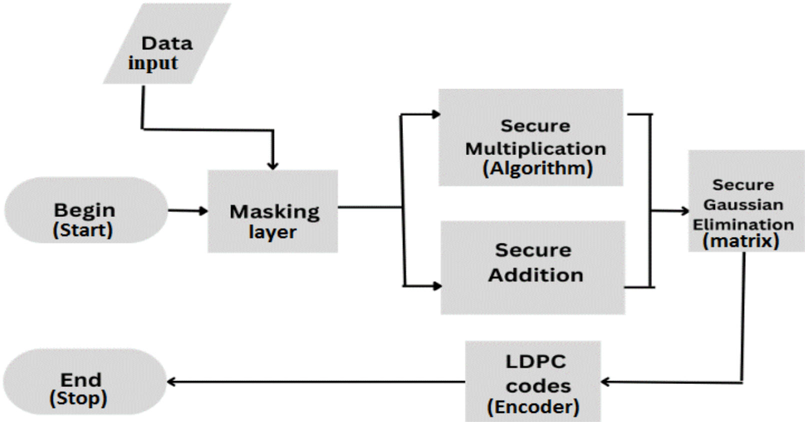

Figure 4. Multiplicative masking method for LDPC codes

3.1.4. Low-density parity check secure coding technique for 5G

The multiplicative masking methods suggest a secure LDPC coding technique for 5G. Data is first encoded to reduce the effect of channel noise. The data must be encrypted using the LDPC encoding procedure for secure transmission. Finite field elements are the first inputs. Once the masking technique has been used, they are encoded using LDPC codes [24]. Lastly, they are decoded based on the LDPC-based decoder. Encoding involves adding several check codes to the data. One of the most significant encoding techniques is called Gaussian elimination [25]-[29].

- The check matrix for LDPC codes is designated as H, which is an M x N matrix.
- M iterations are carried out, where I=M.
- H's i^{th} layer's elements are normalized.
- All components on the lower layers are removed based on the normalizing result.
- $i=i-1$ is computed.
- H is transformed to a lower triangular matrix.

4. RESULTS AND DISCUSSION

In this section, we described the proposed system's simulation and the findings of the study. With a variety of inputs, the procedure is carried out and the associated outputs are obtained in Table 1. Additionally, Figure 5 demonstrates the simulation result of the developed LDPC for 5G. This section provides the experimental results demonstrating the applicability of LDPC security. The low power consumption and delay time as illustrated in Table 1, make the multiplicative masking technique an alternative layer of security to LDPC encoding. Due to the introduction of random masks to the input, before encoding, the LDPC provides better security for communication.

Table 1. Power consumption and delay

Architecture	Power (W)	Delay (ns)
LDPC encoder with multiplicative masking	0.081	105.334

The result obtained in the simulation illustrated in Figure 5 reveals that the LDPC system can be used in communications systems for error correction. Security, power consumption, and delay are the major concerns when using the LDPC for error correction in communication systems. Discuss the security analysis of LDPC codes, focusing on their resistance against various attacks, including information leakage, eavesdropping, or tampering. The study highlighted that the use of multiplicative masking would help to enhance security in communication systems. The proposed multiplicative masking LDPC has also lower power consumption (0.081 Watt), and a lower delay (105.334 milliseconds).

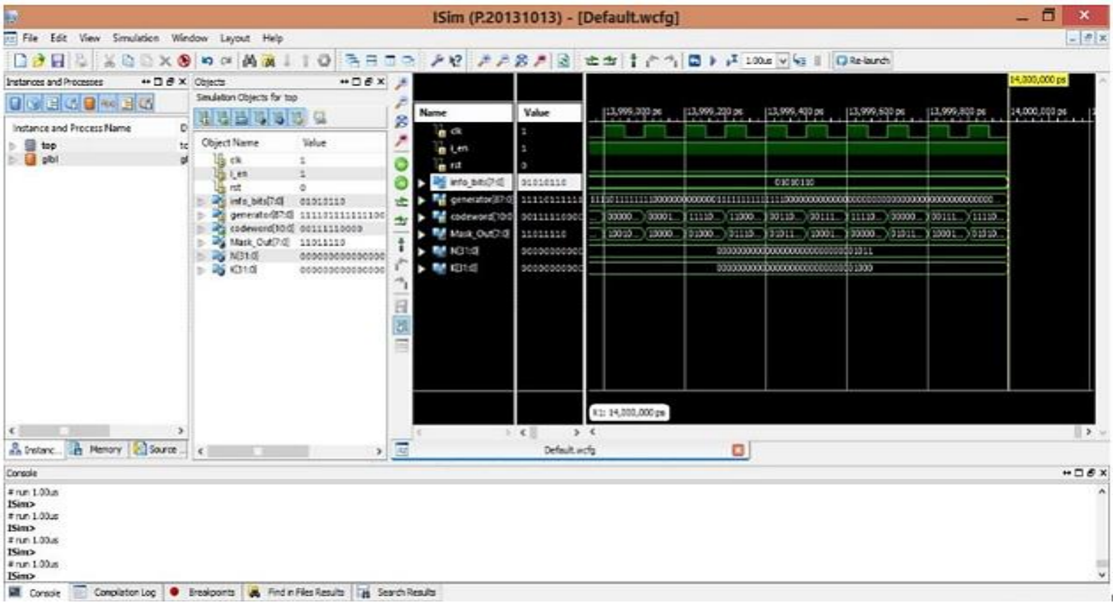

Figure 5. Multiplicative masking method for LDPC codes

5. CONCLUSION

A vast number of individuals use 5G, making it one of the most widely used communication technologies. If 5G has security vulnerabilities, nearly every nation and area in the globe would witness a shift in how communication devices are utilized. The coding of security is an important technological achievement in 5G security. Attackers can easily use the side-channel data that 5G channel coding has disclosed. Although it violates code security, analysis is performed via a side-channel approach. There is presently no systematic research framework in place, and nothing is understood about side-channel attacks on 5G communication devices. Therefore, this paper presents a technique to defend 5G channel coding from side-channel assaults. Three more algorithms are presented which include: multiplication in a finite field, multiplication masks, and LDPC security coding. The recommended solution has been demonstrated to be more secure than the current 5G channel coding. The security coding presented in this study will have an impact on the coding's efficacy. Future research will largely focus on achieving a balance between security and efficacy.

REFERENCES

[1] N. Talati, Z. Wang, and S. Kvatinsky, "Rate-compatible and high-throughput architecture designs for encoding LDPC codes," *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, USA, 2017, pp. 1-4, doi: 10.1109/ISCAS.2017.8050836.

[2] Y. Oohama and B. Santoso, "Information-theoretic security for side-channel attacks to the Shannon cipher system," *arXiv preprint arXiv:1801.02563*, 2018.

[3] Y. Zhang, K. Peng, X. Wang, and J. Song, "Performance Analysis and Code Optimization of IDMA With 5G New Radio LDPC Code," in *IEEE Communications Letters*, vol. 22, no. 8, pp. 1552-1555, Aug. 2018, doi: 10.1109/LCOMM.2018, 2843347.

[4] J. Shi, L. Liu, D. Gündüz, and C. Ling, "Polar Codes and Polar Lattices for the Heegard–Berger Problem," in *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 3760-3771, Sept. 2018, doi: 10.1109/TCOMM.2018.2832618.

[5] X. Wu, M. Jiang, C. Zhao, L. Ma, and Y. Wei, "Low-rate PBRL-LDPC codes for URLLC in 5G," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 800-803, Oct. 2018, doi: 10.1109/LWC.2018.2825988.

[6] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things," in *IEEE Communications Magazine*, vol. 56, no. 2, pp. 60-67, Feb. 2018, doi: 10.1109/MCOM.2018.1700625.

[7] A. Attarkashani, W. Hamouda, J. M. Moualeu, and J. Haghighat, "Performance Analysis of Turbo Codes and Distributed Turbo Codes in Buffer-Aided Relay Systems," in *IEEE Transactions on Communications*, vol. 67, no. 7, pp. 4620-4633, Jul. 2019, doi: 10.1109/TCOMM.2019.2911280.

[8] C. Yang and Y. Guo, "Driftor: mitigating cloud-based side-channel attacks by switching and migrating multi-executor virtual machine," *Frontiers Inf Technol Electronic Eng*., vol. 20, pp. 731–748, 2019, doi: 10.1631/FITEE.1800526.

[9] Z. R. M. Hajiyat, A. Sali, M. Mokhtar, and F. Hashim, "Channel coding scheme for 5g mobile communication system for short length message transmission," *Wireless Personal Communications*, vol. 106, no. 2, pp. 377–400, 2019, doi: 10.1007/s11277-019-06167-7.

[10] X. Sun and I. B. Djordjevic, "FPGA implementation of rate-adaptive spatially coupled LDPC codes suitable for optical communications," *Opt. Express*, vol. 27, pp. 3422-3428, 2019, doi: 10.1364/OE.27.003422.

[11] H. Wu and H. Wang, "A high throughput implementation of QC-LDPC codes for 5G NR," *IEEE Access*, vol. 7, pp. 185373–185384, 2019, doi: 10.1109/ACCESS.2019.2960839.

[12] C. Kun, S. Qi, L. Shengkai, and P. Chengzhi, "Implementation of encoder and decoder for LDPC codes based on FPGA," *Journal of Systems Engineering and Electronics*, vol. 30, no. 4, pp. 642–650, Aug. 2019, doi: 10.21629/JSEE.2019.04.02.

[13] Y. Meng, J. Li, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "Revealing Your Mobile Password via WiFi Signals: Attacks and Countermeasures," in *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 432-449, Feb. 2020, doi: 10.1109/TMC.2019.2893338.

[14] D. Xiao, Z. Gu, C. Yang, and N. Sun, "Data transmission scheme based on AES and polar codes," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 172–177, doi: 10.1109/IWCMC48107.2020.9148558.

[15] D. Čarapić and M. Maksimović, "A comparison of 5G channel coding techniques," *IJEEC-International Journal of Electrical Engineering and Computing*, vol. 4, no. 2, pp. 71–82, 2020, doi: 10.7251/ijeec2002071m.

[16] S. J. Yang, Y. M. Pan, L. Y. Shi, and X. Y. Zhang, "Millimeter-Wave Dual-Polarized Filtering Antenna for 5G Application," in *IEEE Transactions on Antennas and Propagation*, vol. 68, no. 7, pp. 5114–5121, 2020, doi: 10.1109/TAP.2020.2975534.

[17] X. Yao, L. Li, J. Liu, and Q. Li, "A Low Complexity Parallel QC-LDPC Encoder," *2021 IEEE MTT-S International Wireless Symposium (IWS)*, Nanjing, China, 2021, pp. 1–3, doi: 10.1109/IWS52775.2021.9499562.

[18] S. Belhadj, A. M. Lakhdar, and R. I. Bendjillali, "Performance comparison of channel coding schemes for 5G massive machine type communications," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 2, pp. 902–908, 2021, doi: 10.11591/ijeecs.v22.i2.pp902-908.

[19] R. Wang, W. Chen, and C. Han, "Low-complexity encoder implementation for LDPC codes in CCSDS standard," *IEICE Electronics Express*, vol. 18, no. 9, pp. 1–6, 2021, doi: 10.1587/elex.18.20210128.

[20] S. Liao, Y. Zhan, and Z. Shi, "A High Throughput and Flexible Rate 5G NR LDPC Encoder on a Single GPU," *Proceedings of the 2021 23rd International Conference on Advanced Communication Technology (ICACT)*; Pyeongchang, Korea, pp. 29–34, 2021, doi: 10.23919/ICACT51234.2021.9370366.

[21] Y. Zhu, Z. Xing, Z. Li, Y. Zhang, and Y. Hu, "High Area-Efficient Parallel Encoder with Compatible Architecture for 5G LDPC Codes," *Symmetry*, vol. 13, no. 4, p. 700, 2021, doi: 10.3390/sym13040700.

[22] T. T. B. Nguyen, T. N. Tan, and H. Lee, "Low-Complexity High-Throughput QC-LDPC Decoder for 5G New Radio Wireless Communication," *Electronics*, vol. 10, no. 4, pp. 1–18, 2021, doi: 10.3390/electronics10040516.

[23] J. Hyla, W. Sułek, W. Izydorczyk, L. Dziczkowski, and W. Filipowski, "Efficient LDPC Encoder Design for IoT-Type Devices," *Applied Sciences*, vol. 12, no. 5, pp. 25-58, 2022, doi: 10.3390/app12052558.

[24] A. A. Mahmood and A. A. Kadhim, "Joint polar with physical layer network coding and massive multi-input multi-output: performance analysis," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 3, pp. 1469–1476, 2022, doi: 10.11591/ijeecs.v26.i3.pp1469-1476.

[25] A. Aljanabi, O. Alluhaibi, Q. Z. Ahmed, F. A. Khan, Waqas-Bin-Abbas, and P. Lazaridis, "Low complexity single carrier frequency domain detectors for internet of underwater things (IoT)s," *Wireless Personal Communications*, vol. 125, no. 3, pp. 2443–2461, 2022, doi: 10.1007/s11277-022-09667-1.

[26] A. O. Salau, N. Marriwala, and M. Athaee, "Data Security in Wireless Sensor Networks: Attacks and Countermeasures," *Lecture Notes in Networks and Systems*, vol. 140, pp. 173-186, 2021, doi: 10.1007/978-981-15-7130-5_13.

[27] G. G. Gaytare, A. O. Salau, and B. O. Adame, "Interference mitigation technique for self-optimizing Picocell indoor LTE-A networks," *Telecommunication Systems*, vol. 81, pp. 549-560, 2022, doi: 10.1007/s11235-022-00966-3.

[28] B. O. Adame and A. O. Salau, "Genetic Algorithm Based Optimum Finger Selection for Adaptive Minimum Mean Square Error Rake Receivers Discrete Sequence-CDMA Ultra-Wide Band Systems," *Wireless Personal Communication*, vol. 123, pp. 1537–1551, 2022, doi: 10.1007/s11277-021-09199-0.

[29] B. Z. Chekole, A. O. Salau, and H. E. Kassahun, "Multiband Millimeter Wave Phased Array Antenna Design for 5G Communication," *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 106-111, 2022, doi: 10.1109/3ICT56508.2022.9990711.

BIOGRAPHIES OF AUTHORS

Balamurugan Rajangam received an Engineering degree in Electronics and Communication Engineering from Arasu Engineering College in the year 2008. He received a Master's degree in VLSI Design from Kings College of Engineering, Thanjavur, Tamil Nadu, India in 2012. He is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at K. Ramakrishnan College of Engineering, Trichy, India. His areas of interest include VLSI design, IoT and embedded systems, image processing, sensors, and interfacing networks, and the internet of things. He has published 8 articles in peer-reviewed international journals and presented 4 papers in international conferences. He can be contacted at email: balawow@gmail.com.

Manjunathan Alagarsamy received an Engineering degree in Electronics and Communication Engineering from Dr. Navalar Nedunchezhiyan College of Engineering in 2010. He received a Master's degree in Embedded System Technologies from Raja College of Engineering and Technology, Madurai, Tamil Nadu, India in 2013. He is currently working as an Assistant Professor in the Department of Electronics and Communication Engineering at K. Ramakrishnan College of Technology, Trichy, India. His areas of interest include embedded systems, image processing, sensors, interfacing networks, and the Internet of Things. He has published 35 articles in peer-reviewed international journals and presented 7 papers in international conferences. He can be contacted at email: manjunathankrct@gmail.com.

Chirakkal Rathish Radhakrishnan obtained his Bachelor's degree in the field of Electronics and Communication Engineering from Anna University, Chennai, and an M.E in VLSI Design from Karpagam University, Coimbatore. He did his doctorate from St. Peter's Institute of Higher Education and Research, Chennai. He published works in the Proceedings of 18 national and international conferences and has also published 20 articles in well-reputed international journals listed in Scopus and Web of Science. He got 6 national patents with a grant for a design patent. He got several awards from the government for his outrageous service to society. He holds the Guinness record, Tamizhan, and the Asian Book of Records for organizing the World's Largest Students Meet at Codissia, Coimbatore. National Education Brilliance Awards (NEBA), honored him with an International Research Award for the year 2020-2021. He has written 2 books in the title of Artificial Intelligence and Data Warehousing and Data Mining and several book chapters related to the 5G Challenges. Currently, He is an Associate Professor in the Department of Computer Engineering at the New Horizon College of Engineering. He is an active member of the International Association of Engineers (IAENG). He is also serving as a reviewer of an international journal indexed in Scopus Elsevier. His areas of interest include VLSI design, wireless communication, networks, and artificial intelligence. He can be contacted at email: r.rathish87@gmail.com.

Tsehay Admassu Assegie received his M.Sc., in Computer Science from Andhra University, India 2016. He received his B.Sc. in Computer Science from Dilla University, Ethiopia, in 2013. He is Pursuing a Ph.D. in the Department of Electronic and Electrical Engineering, College of IT Engineering, Kyungpook National University, Daegu, Republic of Korea. His research includes biomedical image processing, and the application of machine learning in healthcare. His research has been published in many reputable international journals, and international conferences. He is a member of the International Association of Engineers (IAENG). He has reviewed many papers published in different scientific journals. He is an active reviewer of different reputed journals. Recently, Web of Science has verified 8 peer reviews by him, published in multi-disciplinary digital publishing institute (MDPI) journals. He can be contacted at email: tsehayadmassu2006@gmail.com.

Ayodeji Olalekan Salau received a B.Eng. in Electrical/Computer Engineering from the Federal University of Technology, Minna, Nigeria. He received his M.Sc. and Ph.D. degrees from the Obafemi Awolowo University, Ile-Ife, Nigeria. His research interests include research in the fields of computer vision, image processing, signal processing, machine learning, control systems engineering, and power systems technology. Dr. Salau serves as a reviewer for several reputable international journals. His research has been published in many reputable international conferences, books, and major international journals. He is a registered Engineer with the Council for the Regulation of Engineering in Nigeria (COREN), a member of the International Association of Engineers (IAENG), and a recipient of the Quarterly Franklin Membership with ID number CR32878 given by the Editorial Board of London Journals Press in 2020 for top quality research output. More recently, his research paper was awarded the best paper of the year 2019 in Cogent Engineering. In addition, he is the recipient of the International Research Award on New Science Inventions (NESIN) under the category of "Best Researcher Award" given by Science Father with ID number 9249, 2020. Currently, he works at Afe Babalola University in the Department of Electrical/Electronics and Computer Engineering. He can be contacted at email: ayodejisalau98@gmail.com.

Andrew Quansah is a Ph.D. student in the Department of Electrical and Computer Engineering at the University of North Carolina at Charlotte. He holds an M.Sc. Microelectronics and Wireless Intelligent System from Coventry University in the UK. He received his B.Sc. in Electrical and Electronics Engineering from the Kwame Nkrumah University of Science and Technology. His research interests include advanced embedded systems and computer architecture, wireless communication systems, real-time and application artificial intelligence, and real-time, and embedded operating systems. He can be contacted at email: aquansa1@uncc.edu.

Nur Mohammad Chowdhury is currently pursuing a Ph.D. in Computational Analysis and Modeling at Louisiana Tech University in Ruston, USA. He holds a Master's degree in Information Technology from the University of The West of England (UWE) in Bristol, UK. He also earned his BSc degree in Computer Science and Engineering from Chittagong University of Engineering and Technology, Bangladesh. His diverse academic background reflects his comprehensive understanding of Information Technology and Cyber security. Nur Mohammad's research interests encompass computational intelligence in multimedia processing, real-time data analytics, the internet of things (IoT), machine learning, AI for security, and computer networks in real-time scenarios. His commitment to these fields is evident through his ongoing Ph.D. program, where he engages in advanced research and analysis. He can be contacted at email: nmc026@email.latech.edu.

Ismatul Jannat Chowdhury is currently immersed in the pursuit of a Ph.D. in Electrical Engineering at the esteemed University of North Carolina at Charlotte, USA. Her academic journey encompasses a Master's degree in Data Science from the University of The West of England (UWE) in Bristol, UK, and a Bachelor's degree in Electrical and Electronics Engineering from Premier University, Chittagong, Bangladesh. Her diverse research interests span machine learning and artificial intelligence, data science, optics and photonics, wireless networking, sensing, and security. This broad spectrum reflects her dedication to staying at the forefront of technological advancements. Currently engaged in a Ph.D. program, Ismatul channels his commitment into advanced research and analysis in these cutting-edge fields. She can be contacted at email: ichowdhu@uncc.edu.