Analysis of Security Gaps in 5G Communication using LDPC Codes and NOMA

Vijey Thayananthan
Department of Computer Science
King Abdulaziz University
Jeddah, KSA

ABSTRACT

Advance communication systems such as fifth generation (5G) and 5G+ expect to deploy the security solutions for securing the communication networks. Finding the optimum size of the security gap is a challenging problem in the large scale networks. In this paper, the parity check matrix (H) of low-density parity check (LDPC) considered for determining the security gap is analyzed with the higher rate LDPC coding schemes and different size of frames. Here, optimum LDPC decoding is considered as a method. Especially, the physical layer is investigated with H and two different high-rate codes and simulated to find the optimum size of security gaps for better security. Also, non-orthogonal multiple access (NOMA) is employed to enhance the security solution. Thus, optimum security gap is possible when suitable NOMA is employed in the physical layer of the 5G communication system. As expected in this research conclusion, simulation results show that the security gap decreases when frame size is increased.

General Terms

In this paper, the design of the security gap in the 5G communication channel is considered. Throughout this research, LDPC and NOMA provide optimum security for improving the physical layer of the 5G communication.

Keywords

LDPC coding, Parity check matrix, security gap, NOMA 5G communication.

1. INTRODUCTION

In the 5G communication, providing efficient security solution is one of the main challenges. Although many 5G systems use secure communication channels, security issues such as data breach in public services, malicious attacks in real-time applications, etc. are continuing with evolving threats. Using coding techniques associated with 5G channels could not only detect the error related to the threats of other security issues but also provide the error correction to improve the security levels. The cryptography and information theory involved directly with source and channel coding is being influenced by most of the security issues. As people become a heavy user of mobile communication, they also expect a higher standard of services and applications with maximum privacy and security. These days, communication security prevents unauthorized access and supports for securing the delivery of contents [1].

According to the [2], physical layer security supports to secure the intrinsic randomness of the transmission channel which provides the maximum guarantee of the security in the physical layer. Although many new security issues in 5G wireless communications, physical layer security research are still challengeable with evolving threats. Most of the 5G systems depend on the high throughput which is achievable when LDPC is replaced from existing error control codes. This transition can be ushered for improving security issues such as secrecy rate in 5G communication. Further, LDPC provides many benefits such as block lengths and coding rates, with stringent performance guarantees and minimal description complexity [3]. Over the past decades, multiple accessing techniques have dominated the users' demands. These days, NOMA is playing an important role in many ways to improve the security issues in 5G communication [4]. Further, it supports for improving massive connectivity and high spectral efficiency. Regarding the two-user Gaussian multiple access channel [5], NOMA components in the channel model need the protections to secure the users' multiple access channels.

According to [6], NOMA provides efficient security solutions for securing the physical layer of the 5G channels. Regarding 5G requirements, authors have proposed novel chaos scrambling NOMA. All types of security issues considered in the 5G network and communication are introduced in [7]. They also provide security solutions and policies which secure the 5G systems and architecture. In 5G and 5G+, waveform design, multiple access, and random access techniques depend on the efficient encoding and decoding. Despite many multiple accessing techniques, NOMA is dominating the 5G and 5G+ for securing the communication medium [8].

Although this paper aims to reduce the security gap (SG) which provides secure communication between sender and receiver, NOMA optimize the SG and secrecy capacity to improve LDPC based physical layers. The larger frame size of LDPC code provides better SGs and security regions which helps to provide secure communication and transmission. In the 5G physical layer, NOMA and LDPC provide a better secrecy capacity and SG respectively. In this paper, the utilization of H matrices in high-rate LDPC codes developed for physical channels is considered. In the LDPC coding schemes, random bits in each row are distributed to develop H matrices. It means that an irregular arrangement of non-zero bits is used in each row of the H matrix. Although not as straightforward as in the H matrix development for large scale, irregular LDPC codes are designed with irregular H matrices which are considered with three different sizes.

Shannon also proved that a perfectly secure cipher would use a secret key when the message is encrypted. He did not say what size the key should be. This is rather limiting and optimizing the size of the key because the secret key needs to be transmitted confidentially. In classical cryptography, the size of the secret key is smaller than the message length. Information theory can cover source, channel, and secrecy coding, therefore, it is linked either directly or indirectly with modern cryptography. The cryptography provides secure transmission of messages, texts, images, etc. when more than one person is involved in the communication network. The study of SG based on the LDPC coding scheme provides practical knowledge of implementing a physical layer. Shannon invented a new theory about information theory and cryptography in 1949. Since that, academic and industrial researchers have investigated and demonstrated a number of security algorithms from Shannon's publication [9]. Currently, security issues based on suitable error control coding are focused widely on the physical layers of communication applications. Future computing, medical communication, etc. need an optimum level of security during data transmission. For instance, cloud computing needs a different level of security in each area where cloud service providers use new technology. There are some other applications expected to have a different level of security in each transmission procedure.

The rest of the paper is organized as follows. Section 2 focuses on the background of LDPC coding and its general properties used in the physical layer. Section 3 provides cryptography and LDPC coding with proposed schemes handled with the random approach of H matrices and different coding rate of LDPC schemes. It also describes the security issues of 5G network communication and infrastructure which includes the 5G channels. Section 4 explains the details of security levels and regions where SGs need to be measured for analyzing security performance of 5G communication. Section 5 explains the SG limitations and trade-offs between bit error performance and design complexity. In Section 6; overall conclusions are written based on the theoretical analysis and results.

2. BACKGROUND

The original design of LDPC coding was discovered by a Gallager [10] in 1962. Although it has the same concept as a linear block code, the H matrix of the LDPC should have a low density of ones. In the LDPC, message and code lengths are considered as K and N respectively. Throughout this research paper, the sizes of H and generator matrices are (N–K)×N and K×N. Generator matrix G, which generates N bits code-word from the K information bits. There are two types of LDPC codes contained with regular and irregular H matrices [11]. If a constant number of 1s (ones) are used in each row and column of the H matrix, it can be called regular LDPC codes. If each row and column of the H matrix is not constant, it can be called irregular LDPC codes. The received code-word from the NOMA based encoding is sent through NOMA based decoding. Finally, each code-word is decoded by (N–K) check nodes designed in the LDPC decoder. Although different code rates defined as K/N considered for analyzing SGs, a number of ones in H matrices should be considered carefully. Also, redundant bits (N-K) of LDPC have been used to detect and correct the errors.

Few selected high rate codes have been simulated and analyzed the performance, which closes to the Shannon theory [12, 13]. Davey and Mackay first investigated the extension of LDPC with non-binary inputs. He simulated non-binary Galois field GF(q) and proved that the performance of non-binary LDPC should be better than binary LDPC. In his simulation, additive-white-Gaussian-noise (AWGN) channel is used in the physical layer development. In this paper, binary inputs have been used to implement security.

2.1 LDPC and Parity Check Matrix

As mentioned in section A, Gallager created the H matrix slightly different way where he used a number of sub-matrices [14]. Here, row weight is greater than 1, and the column weight is fixed as 1. The LDPC code is one of the error-correcting control codes determined by an H matrix which takes the particular form of a dimension M×N. Such a matrix is given as in (1)

$H \in GF(2)^{MN}$
(1)

More specifically, LDPC code is characterized by the proportion of nonzero entities in each row and each column of H matrices. Following two equations (2) and (3) are used to summarise row and column of the polynomials.

$A(x) = \sum_{k}^{d_v} A_k x^k$
(2)

$B(x) = \sum_{k}^{d_c} B_k x^k$
(3)

Above polynomial equations (2) and (3) indicate the proportion of nonzero entities in the columns or rows H matrix and, d_v *and* d_c denotes the maximum *variable* node (v) degree and check node (*c*) degree respectively.

$A_k = N^{-1}|\{j:\ column\ \ H_j\ \ 1_r\ \ 1 \le r \le k\}|$
(4)

$B_k = M^{-1}|\{i:\ \ row\ \ H_i\ \ 1_r\ \ 1 \le r \le k\}|$
(5)

Equations (4) and (5) are representing columns and rows which contains k ones respectively. These random ones are arranged in irregular order. Here, total weight is considered as adding all ones in each row or column. It helps to detect and correct the error in each frame. SG is also depended on this total weight which could be changed according to the security level applications need.

For LDPC code with polynomials A(x) and B(x), the H matrix contains a total of Z(N) which is same as Z(M) as provided in (6) and (7) respectively.

$$Z(N) = N \sum_{k}^{d_v} k A_k \qquad (6)$$

$$Z(M) = M \sum_{k}^{d_c} k B_k \qquad (7)$$

Here, nonzero entries are used to calculate the total of each (6) and (7).

This number Z(N) grows only proportionally to the block size N, whereas a randomly chosen matrix H would contain a quadratic number of nonzero entries (i.e., assuming that M is proportional to N).

With the matrix size is fixed, all the LDPC codes characterized by the same polynomials A(x) and B(x) have pretty much the same properties. Hence, it is sufficient for our purposes to think of an LDPC code as being randomly chosen among an ensemble; with overwhelming probability, such a code will be as strong as any other code in the ensemble.

2.2 Decoding of LDPC Scheme

There are a number of different decoding techniques [15, 16] used in LDPC decoding developments. In this paper, the decoding technique involved with iteration approach. In order to decode the encoded word from the noisy channel, the number of iterations can be increased. To prevent Eve's involvement, increasing iteration would be one of the options which create the confusions. The decoding procedures of LDPC mainly depend on the variable and check nodes where messages are exchanged. In order to decode the encoded code word, Belief Propagation decoding algorithm [17] is chosen in this research. In this research, soft decision decoding is developed for improving bit error performance.

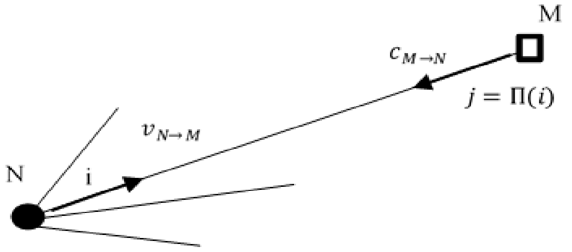

Fig 1: Edges of the Tanner graph

In Fig. 1, the circulation of the messages on edge is shown and connections. An edge (or connection) can be defined in two ways. Here, i and j are linked by formula, $j = \Pi(i)$ where Π is a bijective function. In the Tanner graph, the bit connections can be numbered by i going from 1 to M (or from 0 to M-1); and same for the check connections with j. Exact values of M and other details are given in the following section.

First, the check node is updated with noisy value y sent by a variable node (N) to its adjacent check node (M). Then check node sends value x (assume x may be different or equal to y) back to the variable node. At this variable node is updated with the accurate value of x which is a log likelihood ratio of X. In (8), Pr represents the probability. In the first step, the variable node v_j knows only y_j. Thus, accuan rate value is calculated as:

$$A_{v_j\to c} = A(X_j \Big| Y_j) = ln\frac{Pr[X_j=0, Y_j=y_j]}{Pr[X_j=1, Y_j=y_j]} \quad (8)$$

It is propagated to check node and updated the check node. Then the variable node is updated with the new value. This process (8) is continued until the end of the iteration which is fixed according to code rates and frame sizes.

2.3 Security Issues in 5G

The main objective of this section is to explain why security is important to 5G and how it is different when LDPC and NOMA are employed to analyze the secrecy rate and SGs. Further, security issues of 5G are considered as an evolving security solution which is dynamic and different from previous generations (2G/3G/4G) considered with orthogonal multiple access. According to the [18], the performance analysis and code optimization of interleave-division multiple access (IDMA) can be achievable with the rate-compatible LDPC code. This type of code not only improve the performance of 5G new radio but also increase the secrecy rate. Here, authors employed the combination of multi-edge type density evolution and extrinsic information transfer.

A combining non-binary (NB) LDPC sachem is considered with higher order modulation and probabilistic amplitude shaping (PAS). Despite many LDPC decoding approaches, a bit-metric decoder is used for increasing the flexibility of the coding scheme used in the 5G environment. Here, PAS supports to improve security without loss of performance [19]. As described in [20], a two-layer architecture vision is introduced to address the challenges considered in 5G mobile networks. Although this architecture contains a radio network and a network cloud, it is integrated with various enablers such as small cells, massive MIMO, control/user (C/U)-plane split, NFV, and SDN. According to [21], the Gaussian wiretap channel is considered for securing the transmission which uses the LDPC codes with granular Hybrid Automatic Repeat reQuest (HARQ) protocol. In this wiretap channel, HARQ granularity not only provides efficient decoding with minimum rate but also secure the transmission with minimum information leakage that may benefit to eavesdropping. In [22], the authors proposed a feedback method combined with LDPC. It provides strong and unconditional security using soft decision decoding of LDPC. Also, it establishes the efficient wiretap channels for improving both the binary symmetric channel and binary input additive white Gaussian noise channel. Use of LDPC in wiretap channel improve authentication scheme proposed in [23]. In this scheme, ϵ-AU 2 hash functions are employed with LDPC over binary-input wiretap channel.

Although the high speeds and low latency are expected in millimeter wave (mmWave) communications, LDPC plays an important role to improve the channel conditions. In mmWave, channel conditions influence to beam alignment, blockage, and interference depend on the modulation size, coding rate and other transmission parameters [24]. Although Turbo codes have enough error correcting capabilities, LDPC dominates the 5G and beyond. Further, LDPC codes are near the Shannon limit which improves the error performance secrecy rate and SG in 5G communication [25].

3. CRYPTOGRAPHY AND CODING

In this section, two different coding rates are considered for investigating SGs. According to theory, LDPC based crypto-coding design with different decoding algorithms and its basic properties such as coding rate, error correcting capability, etc. vary the SGs. Attack and some kind of interaction between the sender and receiver are some examples of the growing problems in the modern communication system. Channel must be protected from these attackers who should be confused or delayed using new cryptographic techniques. Coding and cryptographic techniques provide the number of advantages in channel developments for securing transmission. There are many techniques used in the number of a different situation where communication system depends on the applications. Whatever situation, attackers' involvement must be removed. Researchers are still investigating and suggesting alternative solutions and algorithms solve these problems.

3.1 Cryptography and coding for security

Although many coding techniques provide necessary support to improve the security levels in 5G communication, variable rate of LDPC coding techniques increases the secrecy rates of the physical layer. All cryptography and coding techniques between the source and destination provide the necessary security solutions. In the physical layer, channel coding uses the appropriate coding techniques, secrecy coding known as cryptography and noise model involved with the medium. As far as the secrecy rate is concerned, efficient cryptography should be employed to improve the confidentiality, data integrity, authentication, and non–repudiation which is desired properties of cryptography.

As indicated in [26], punctured coding techniques provide many benefits to secure the physical layer of the LDPC based communication channels. Although it increases the coding rate of the LDPC design, it reduces the SG which is the key idea of this paper. In this research, different frame sizes of LDPC could be designed for analyzing the SG. Further, employing NOMA optimizes the secrecy rate of the channel. These secrecy rate and SG are key parameters to improve the security levels of the 5G communication. Definition of the secrecy rate is that length of the encoded codeword divides the length of the secret message. In this paper, selected higher rate codes are chosen to show improvement in the SG. H matrix is also developed randomly to improve the complexity which will reduce the SG further. Implementing such H matrices is exceptionally difficult, but the optimum density of the H matrix would be extremely useful for security.

Security is designed and implemented according to the applications. For instance, mobile digital video transmission over the wireless networks needs some security which is varied with variable rates. If an application is involved with a fixed rate, security can be designed with a fixed rate. In this research, rates of the LDPC code and their SGs are investigated with random H matrices. These SGs will be varied with the length of the LDPC codes depend on the length of the frames which are 4k, 16k, and 64k. When the length of the code is medium to high, the level of security could be better and implemented according to the applications [27].

In coding and cryptographic concept, the key generation that helps to develop public and private key, encryption and decryption algorithms are explained with error-correcting coding. The public key developments rely on coding parameters such as code length N, message length K and error-correcting capability t which means that code can correct up to t errors. When a message is encrypted, parity bits are added based on Hamming weight wH(e) ≤ t. Galois field based on, order m and t of the code are important parameters in the coding scheme and cryptography.

3.2 Design procedures of cryptography

In this section, actual message length (assume m = 2k bits) is considered as the input of the LDPC encoder. Before the encoding, the actual message is distributed within K, which is the length of the information frame (K > m) in LDPC. The message can be extended to K bits frame using a known bit pattern. Then, it is encoded using the LDPC encoding technique. Here, the length of the LDPC encoder is N considered with three cases such as 4k, 16k, and 64k. For instance, the 64k frame is considered where m = 2k bits message is hidden within the large frame. Real message (m) can be located randomly in the 64k frame. Secret location and known bit pattern must be shared by Alice and Bob when they want to exchange messages. In this analysis, messages with 4k or smaller than 4k messages could be used.

LDPC allows us to design a flexible coding scheme with different H matrices. It means that different frame sizes used in this research are considered to verify the SGs. They do not only depend on the frame sizes but also influence H matrix designs. In order to investigate the security issues based on the SGs, two different coding rates are focused on different frame sizes. In this paper, the irregular LDPC code is designed with the following parameters. The (N, K) LDPC codes are block codes defined by the H matrices (i.e., sparse), where N and K are coded, and data block sizes respectively. A regular H matrix exactly has j ones in each column, and i ones in each row, where j < i, and both are small compared to N. An irregular H matrix is still sparse, but not all the rows and columns contain same a number of ones

3.3 Design procedures for 4k, 16k, and 64k

In this section, the details of design procedures are considered with higher rates of LDPC scheme. In this proposal, 4k, 16k, and 64k frame sizes are used as lengths of encoders. Information bits of the 4k case can be used within 16k, and 64k cases but fixed and selected bits or known bits patterns have to be added in front or at the back of the 4k frame. For instances, the 16k frame needs extra 12k known bits or some known pattern of bits. It is not difficult, but synchronization or, pattern should be known by both Alice and Bob. Table 1 shows the design details of higher rate codes. Here, secrecy capacity can be defined as the highest transmission rate Bob can achieve through the C1 receiver.

Table 1. LDPC Code Parameters for proposed code rates

Frame size	RATE = 0.9		RATE = 0.95	
	K	N	K	N
64k	58320	64800	61560	64800
16k	14580	16200	15390	16200
4k	3645	4050	3876	4080

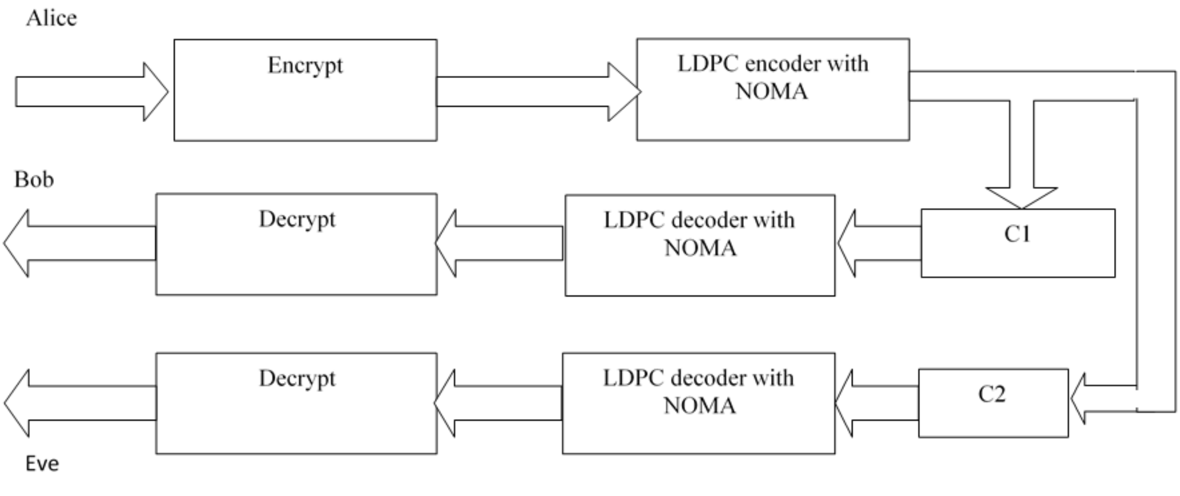

Fig 2: The proposed model with LDPC coding scheme and NOMA for measuring SG

As shown in Fig. 2, security levels of the channels C1 and C2 can be compared. When Bob and Eve use the channels C1 and C2 for receiving messages, security levels of these channels need to be considered with different channel conditions [28]. Secrecy capacity of each channel can be improved through which different types of NOMA are employed to change the channel conditions. Despite many types of NOMA, coding parameters of LDPC scheme enhances the secrecy capacity through the appropriate NOMA. When C2 has a higher secrecy capacity than the C1, Bob will receive a secure message. The main objective of this research is to explain why security is fundamental to 5G and how it is improved when NOMA is employed in the LDPC based channel coding. This novel approach of security solution in 5G is different from which 2G/3G/4G securities involve.

In the large scale or complex networks, the concepts of physical layer security provide reasonable secrecy capacity and SGs to improve security solutions. Hence, enhancing secrecy capacity and reducing SG is inevitable in 5G networks because 5G communication is merging with large scale and complex networks. Thus, 5G NOMA is employed to enhance security solutions.

4. RESULTS AND ANALYSIS

As mentioned in the previous sections, H matrices and frame sizes are developed and added within the full LDPC program which contains encoder, decoder, and AWGN. All cases were implemented using C programming and simulated to verify the SGs. In this research, minimum mean-square error with successive interference cancellation (MMSE-SIC) is used in NOMA based receiver for improving receiver performance which are secrecy rate, throughput, etc. During the decoding, LDPC decoding algorithm used in this simulation takes a number of iterations which reduce the SG as well as error corrections, so Bob and Alice should have such details. If Bob knows a correct number of iteration used for decoding, Eve cannot decode the message within the time. As shown in Fig. 3, the SG of the 4k, 16k, and 64k codes are investigated with minimum and maximum levels of security. High-rate and code lengths are useful parameters in the coding and cryptography. When the length of the code is increased, level of the security is reduced.

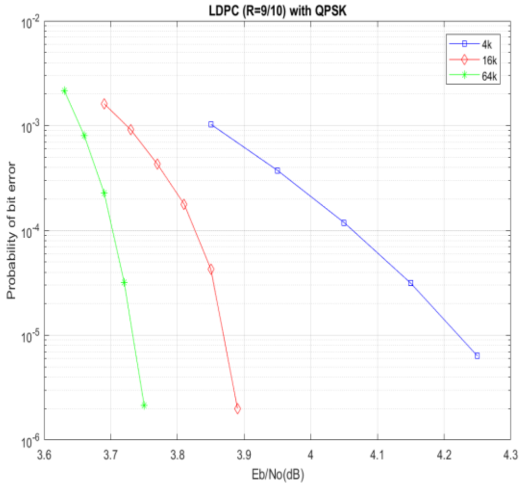

Fig 3: BER vs. Eb/No performance of LDPC with R=0.9

From the previous papers [29], the SG is measured for different coding schemes. As mentioned in [27], the punctured technique is better to reduce the SG and complexity. According to those papers, the SG was investigated with some code rates (up to 0.7). In this paper, high-rate codes are simulated to prove that the SG was decreasing when frame size increased. In addition to this, errors, complexity, and iteration are purposely increased to confuse Eve, but still, the SG is reduced with frame size.

Where Mod and R are QPSK symbol (2bits) and code rate respectively. In this paper, the main focus of the research is the SG, which helps to improve the security between source and destination. For instance, Alice and Bob have secure communication. Still, Eve may enter, but chances are less. As shown in Fig. 4, the SGs for 4k, 16k and 64k code are about 5.88dB, 5.6dB, and 5.35dB respectively.

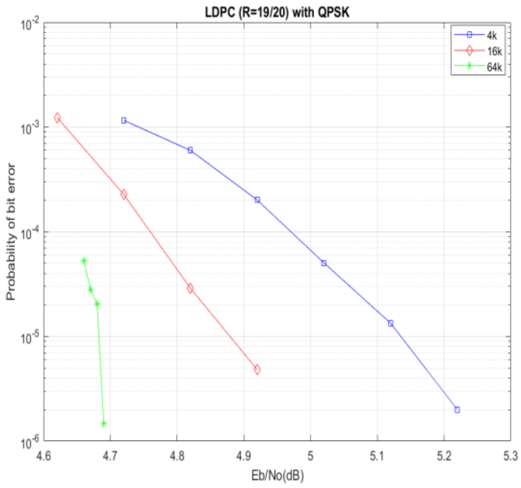

Fig 4: BER vs. Eb/No performance of LDPC with R=0.95

Although simulations are completed to analyze the SG with NOMA and without NOMA, results were varied with frame size. When NOMA allows the 5G system to increase users' multiple access channel, the security of each channel should be enhanced with the optimum SGs and secrecy capacity. These security parameters are important for analyzing security keys influenced to a permutation which creates the cipher bits. When permutations are very high, finding private keys is very difficult. This is one of the advantages when higher rate coding is employed in the security analysis. However, some attackers decode the message and key after the continuous try of revealing the error vector which provides necessary information. From Fig. 3 and Fig. 4, the SGs can be calculated for each frame size as given in Table 2. In [27], SNR values used in the horizontal axis were recorded to determine the SG. The relationship between the SNR and Eb/No is given in equation (9).

$$SNR = \frac{Eb}{No} + 10\log(Mod \times R) \qquad (9)$$

Here, the error floor of the 4k simulation shown in Fig.3 and Fig. 4 is also reduced, but the SG is increasing with code rates because maximum value, is increased with the code rates. From Table 2, SGs can be calculated for each case as given below

$$SG = \left(\frac{Eb}{No}\right)_{min} - \left(\frac{Eb}{No}\right)_{max} \qquad (10)$$

In (10), minimum (min) and maximum (max) points can be obtained from any BER graphs. In the simulated graphs (Fig. 3 and Fig. 4), the maximum value is not shown (not drawn) because the probability of bit error is varied between 0.3 and 0.9. Although the SG depends on frame size, following conditions provide the relationships between the secrecy rate and SG. They are $R > R_s$ and $N > K_s$, where R_s and K_s are secrecy rate and length of the smallest secret message respectively. When the above conditions are executed in the 5G channels, future 5G physical layer will achieve the better security performance in the large scale networks and other 5G systems.

Table 2. The SG analysis of the proposed scheme

Frame size	Security levels	Security regions (dB)	
		0.9	**0.95**
4k	Minimum	4.25	5.22
	Maximum	-0.1	-0.66
	SG with LDPC	4.35	5.88
	SG (LDPC+NOMA)	4.23	5.74
16k	Minimum	3.9	4.92
	Maximum	-0.07	-0.68
	SG with LDPC	3.97	5.6
	SG (LDPC+NOMA)	3.82	4.96
64k	Minimum	3.75	4.69
	Maximum	-0.08	-0.66
	SG with LDPC	3.83	5.35
	SG (LDPC+NOMA)	3.71	5.23

The SG of the physical layer channel not only depends on the parameters of the LDPC coding but also the benefits of NOMA. Here, the SG improves the security of the 5G physical layers (5G communication channels) between the source and destination. Although SG with LDPC and NOMA provides a slight improvement, the secrecy rate of the physical layer can be increased by the correct type of NOMA [30].

5. SECURITY AND PERFORMANCE

The LDPC coding schemes offer superior coding gain which provides SGs where the minimum and maximum security levels are identified.

With the H matrix developments of LDPC, BER vs. Eb/No performance has been analyzed for different coding rates. Coding scheme with larger block size provides extra coding gain in the lower bit error rate (10e-6 < BER < 10e-10), which makes a power-efficient system and enables to achieve higher data rates between 50Mbps and 100Mbps. The extra coding gain and SG obtained in this research are used in the following ways.

- To confuse the eavesdroppers' attacks with different secrecy rate which provides different behavior of the channel
- To use different error-correcting capability which helps increase the error in Eve's channel
- To minimize the SG and increase the security region

Although the SG depends on the channel models, NOMA plays an important role to improve security levels of the 5G based physical layers. In a real environment, finding error-free public channels is not easy for sending and receiving messages or transferring data and files. According to the properties of NOMA, network secrecy capacity can be improved for securing 5G channels and infrastructure. Secrecy capacity is the key element for securing 5G network communication. All emerging technologies such as IoT based 5G influences to secrecy rate which could be set using efficient cryptography and coding.

Table 3. Comparisons of security performance

Rate	LDPC	LDPC with NOMA
0.9	3.9 < SG < 4.2	3.7 < SG < 4.0
0.95	5.4 < SG < 5.9	5.3 < SG < 5.7

As shown in table 3, the best SG can be selected as a security range. Security performance depends on the secrecy rate, SG and complexity. In the lower bit error rate (BER), error floor is created in LDPC schemes. The error floor can be minimized using outer coding such as Reed Solomon. Although NOMA supports to improve the SG, outer coding should be employed to enhance the overall security performance. Simulation results justify that our proposed opportunistic NOMA scheme can significantly improve the network throughput and secrecy capacity in many scenarios.

5.1 Performance for selected LDPC codes

The LDPC schemes with selected code rates 0.9 and 0.95 have been simulated to investigate the level of security and BER performance in QPSK modulation. Although 4k, 16k and 64 LDPC schemes have been simulated, the optimum size should be depending on the security needed for the particular application. In addition to this, LDPC and its properties will provide better security to a different channel which may be employed to different applications.

The optimization of BER performance against the frame size is investigated. Although the complexity analysis of H matrices is important, selected H matrices used in this research are briefly considered. In order to achieve optimal results, the numbers of irregular H matrices have been designed and tested. From the design parameters, the BER performance improvement against complexity reduction is noted in a coding scheme because the SG is depended on the coding parameters.

The H matrices with less number of non zero bits (ones) reduce the complexity with BER performance degradation. In order to achieve optimum BER performance, irregular H matrices should be designed with a reasonable number of 1s (digits of one). It may be depending on other LDPC parameters too. The error-correcting capability of the LDPC scheme increases with row weight increments of the H matrices, which provides more coding gain in the BER performance. The error-correcting capability of LDPC and H matrices of the LDPC influences with security properties indirectly.

5.2 Computational complexity and security

The variable coding rate of the LDPC scheme can be achieved without modifying hardware. Further, this development implemented with puncturing technique reduces the complexity. In this paper, different H matrices are used according to the frame sizes could be applied to verify the level of the SGs which are useful to identify the secure regions and reliable regions in future applications. In this scheme, H matrices are developed with a random approach, so hardware implementation should be complicated. Each development of H matrix would take different complexities because it is depended on the column weights. For instance, high security needs H matrices with complex design, large frame size, etc. In this research, H matrix properties used to analyze the LDPC code structure, and its complexity is important in security development. Row and columns are investigated for selected LDPC coding schemes where properties of H matrix are designed as regular LDPC codes. Although applications of regular and irregular H matrices are the same, the complexity of matrices in the system will be different. This property is invariant by permutation as mentioned [31].

In this analysis, the physical layer security and NOMA can be considered for securing large-scale networks. In the 5G based physical layer, the secrecy outage probability defines the protected zone. When it decreases, the radius of the protected zone increases with the types of NOMA. Although the SG of the LDPC coding depends on the complexity, secrecy rate depends on the types of NOMA in the receiver and their complexity. Regarding the secrecy rate, 5G based physical layer uses the MMSE-SIC which is one of the receiver algorithms. It calculates the complexity as below.

$$Complexity = O(N_{Rx}^3 SF^3 N_U) \qquad (11)$$

In (11), $SF, N_{Rx}\ and\ N_U$ represent the spreading length, the number of receiver antennas and users respectively. Combining cryptographic and coding (crypto-coding) not only enhances security solutions but also reduces the computational cost. Using the best H matrices of LDPC coding, best security solutions can be implemented. Although the H matrix influences the complexity of the crypto-coding implementation, it improves the secrecy capacity and SG. In this analysis, LDPC decoding uses the 6 bits operation which improves the SG and secrecy capacity. When LDPC uses more than 6 bits operations, crypto-coding provides a better SG and secrecy capacity at the expenses of hardware costs. It means that hardware complexity increases when 8 bits operations are used to improve the SG.

In H matrix based on random approach, column weight and row weight are fixed according to the applications, but 1s in each row distributed randomly. Complexity may be higher than expected, but a secure channel could be designed with a secure key. The knowledge of the secret key must be very important to recover the message.

6. CONCLUSIONS

Through this research, SGs are reduced when frame sizes are increased. The optimum size for SGs in future cryptography could be achieved between the medium and large size. In order to improve security in the physical layer, the design of high rate LDPC codes with the largest frame size would be better because it reduces the SGs. According to the theoretical analysis, NOMA increases secrecy capacity in 5G physical layer channels designed with LDPC scheme. In this research, the NOMA approach allows the 5G to enhance the overall security solutions. Although NOMA does not involve the SG improvement directly, it provides the optimization to enhance the SG through the secrecy rate. In the 5G system, NOMA not only enhances the secrecy capacity but also improve the secrecy rate could be optimized through the appropriate version of the NOMA. In order to achieve the extra security and increase the error corrections in the physical layer, the actual message can be located randomly within the largest frame. The LDPC scheme with larger than 64k block size provides better BER performance as well as SG. Thus, LDPC and NOMA will provide better security solutions in the large scale networks of 5G communication. According to [32], the future work of the SG will be analyzed with different types of NOMA and other accessing techniques employed in 6G communication.

7. ACKNOWLEDGMENTS

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah. The author, therefore, acknowledge with thanks, DSR technical and financial support.

8. REFERENCES

[1] Sriram, Poorna Pravallika, Hwang-Cheng Wang, Hema Ganesh Jami, and Kathiravan Srinivasan. "5G Security: Concepts and Challenges." In *5G Enabled Secure Wireless Networks*, pp. 1-43. Springer, Cham, 2019.

[2] Wu, Yongpeng, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong, and Xiqi Gao. "A survey of physical layer security techniques for 5G wireless networks and challenges ahead." *IEEE Journal on Selected Areas in Communications* 36, no. 4 (2018): 679-695.

[3] Richardson, Tom, and Shrinivas Kudekar. "Design of low-density parity-check codes for a 5G new radio." *IEEE Communications Magazine* 56, no. 3 (2018): 28-34.

[4] Liu, Yuanwei, Zhijin Qin, Maged Elkashlan, Zhiguo Ding, Arumugam Nallanathan, and Lajos Hanzo. "Non-orthogonal multiple access for 5G and beyond." *arXiv preprint arXiv:1808.00277* (2018).

[5] Chen, Shuang, Kewu Peng, Yushu Zhang, and Jian Song. "Near capacity LDPC coded MU-BICM-ID for 5G." In 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1418-1423. IEEE, 2015.

[6] Shao, Xuanbo, and Zhanji Wu. "A Novel Multiple Access Scheme with Physical Layer Security." In *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pp. 36-40. IEEE, 2018.

[7] Jayakody, Dushantha Nalin K., Kathiravan Srinivasan, and Vishal Sharma. "5G Enabled Secure Wireless Networks." (2019).

[8] Vaezi, Mojtaba, Zhiguo Ding, and H. Vincent Poor. "Multiple Access Techniques for 5G Wireless Networks and Beyond." (2018).

[9] E. Shannon, “Communication theory of secrecy systems,” B.S.T.J., vol. 28, pp. 656–715, Oct. 1949.

[10] R. G. Gallager, “Low-Density Parity-check Codes,” IRE Trans. Inform. Theory, vol. IT-8, pp. 21-28, Jan. 1962.

[11] O. Hamdi, M. Abdelhedi, A. Bouallegue & S. Harari, Weakness on Cryptographic schemes based on regular LDPC codes. International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, 2010.

[12] S. Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, “On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit, “ IEEE Commun. Lett. vol. 5, pp. 58-60, Feb 2001.

[13] J. C. Mackay,"Near Shannon limit performance of low-density parity-check codes" Electron. Lett., vol. 33, pp. 457–458, Mars. 1997.

[14] J. Muramatsu, T. Uyematsu, and T. Wadayama, "Low-density parity check matrices for coding correlated sources," IEEE Trans. Inform — Theory, 51, 3645 – 3654, 2005.

[15] D. Liveris, Z. Xiong and C. N. Georghiades, compression of binary sources with side information at the decoder using LDPC codes, IEEE Commun. Lett. vol. 6, pp. 440-442, 2002.

[16] R.Lucas, M. Fossorier, Y. Kou, and S. Lin, "Iterative decoding of one-step majority-logic decodable codes based on belief propagation, " IEEE Trans. Comm., pp 931-937, June 2000.

[17] J. Chen and M. P. C. Fossorier, "Near optimum universal belief propagation based decoding of Low-Density Parity-Check Codes" IEEE Transactions on Communications, vol. 50, pp. 406–414, March 2002.

[18] Zhang, Yushu, Kewu Peng, Xianbin Wang, and Jian Song. "Performance Analysis and Code Optimization of IDMA with 5G New Radio LDPC Code." IEEE Communications Letters (2018).

[19] Steiner F, Böcherer G, Liva G. Bit-Metric Decoding of Non-Binary LDPC Codes with Probabilistic Amplitude Shaping. arXiv preprint arXiv:1809.04037. 2018 Sep 11.

[20] Agyapong, P.K.; Iwamura, M.; Staehle, D.; Kiess, W.; Benjebbour, A. Design Considerations for a 5G Network Architecture. IEEE Commun. Mag. 2014, 52, 65–75.

[21] Taieb, Mohamed Haj, and Jean-Yves Chouinard. "Reliable and secure communications over Gaussian wiretap channel using HARQ LDPC codes and error contamination." In *2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 158-163. IEEE, 2015.

[22] Zhang, Gaoyuan, Hong Wen, Jiexin Pu, and Jie Tang. "Build-in wiretap channel I with feedback and LDPC codes by soft decision decoding." IET Communications 11, no. 11 (2017): 1808-1814.

[23] Chen, Dajiang, Ning Zhang, Rongxing Lu, Xiaojie Fang, Kuan Zhang, Zhiguang Qin, and Xuemin Shen. "An LDPC code based physical layer message authentication scheme with perfect security." IEEE Journal on Selected Areas in Communications 36, no. 4 (2018): 748-761.

[24] Song, Jiho, Borja Peleato, David J. Love, Tianqiong Luo, Dennis Ogbe, and Amitava Ghosh. "Optimizing incremental redundancy for millimeter wave wireless communication using low-density parity check codes." (2017).

[25] Shah, Pradeep M., Prakash D. Vyavahare, and Anjana Jain. "Modern error correcting codes for 4G and beyond: Turbo codes and LDPC codes." In *2015 Radio and Antenna Days of the Indian Ocean (RADIO)*, pp. 1-2. IEEE, 2015.

[26] P. Fewer, M. F. Flanagan & A. D. Fagan, *A Versatile Variable Rate LDPC Codec Architecture.* IEEE Trans. on Circuits and system —I Regular paper, VOL. 54, NO. 10, 2007.

[27] Klinc, J. Ha, S. W. McLaughlin, J. Barros & B. J. Kwak, LDPC Codes for Physical Layer Security. USA and Korea: IEEE "GLOBECOM" 2009 proceedings, 2009.

[28] W. K. Harrison & S. W. McLaughlin, Physical-Layer Security: Combining Error Control Coding and Cryptography. School of ECE, Georgia Institute of Technology, Atlanta, GA.: IEEE International Conference on Communications, 2009.

[29] B. Kwak∗, N. Song†, B. Park∗, D. Klinc‡ and S. W. McLaughlin, "Physical Layer Security with Yarg Code, " First International Conference on Emerging Network Intelligence, The IEEE Computer Society, 2009.

[30] Wang, Yingmin, Bin Ren, Shaohui Sun, Shaoli Kang, and Xinwei Yue. "Analysis of non-orthogonal multiple access for 5G." China Communications 13, no. 2 (2016): 52-66.

[31] T. Richardson, A. Shokrollahi and. R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," IEEE Trans. Inform. Theory, vol. 47, pp. 619–637, Feb. 2001.

[32] Al-Eryani, Yasser, and Ekram Hossain. "Delta-OMA (D-OMA): A New Method for Massive Multiple Access in 6G." arXiv preprint arXiv:1901.07100 (2019).