Journal of Electrical and Electronic Engineering
2019; 7(6): 134-142
http://www.sciencepublishinggroup.com/j/jeee
doi: 10.11648/j.jeee.20190706.11
ISSN: 2329-1613 (Print); ISSN: 2329-1605 (Online)

Invited Paper: Raptor Code and Massive MiMo for Secure Wireless Delivery in 5G

Djedjiga Benzid*, Michel Kadoch

Department of Electrical Engineering, École de Technologie Supérieure, Montreal, Canada

Email address:
Djedjiga.benzid.1@ens.etsmtl.ca (D. Benzid), michel.kadoch@etsmtl.ca (M. Kadoch)

*Corresponding author

To cite this article:
Djedjiga Benzid, Michel Kadoch. Invited Paper: Raptor Code and Massive MiMo for Secure Wireless Delivery in 5G. *Journal of Electrical and Electronic Engineering*. Vol. 7, No. 6, 2019, pp. 134-142. doi: 10.11648/j.jeee.20190706.11

Received: September 3, 2019; **Accepted**: October 4, 2019; **Published**: November 27, 2019

Abstract: Based on broadcast transmission, the future Fifth-Generation networks, 5G, suffer from a critical threat, which is the eavesdropping. This issue can be fixed with the cryptographic protocols. Nevertheless, this method is complex and challenging because of the active topology of wireless networks, which does not permit effective management of security keys. Recently, Physical Layer Security (PLS) method is applied as an alternative solution to mitigate the privacy problem, where the characteristic of the physical layer schemes, namely the modulation, Massive Multi-Input Multi-Output (m-MiMo) and channel coding are exploited to ensure privacy. The fountain code is one of these methods where the legitimate receiver must recover the message before eavesdropper did. However, this feature cannot be exploited in 5G networks in the presence of an intruder using the m-MiMo. Furthermore, the design of Artificial Noise (AN) needed in m-MiMo involves a computational complexity and excessive consumption of energy that complicate the secrecy management for fountain code. In this article, we propose a new method to avoid this problem by judiciously exploiting the features of both technologies. The new approach uses the Raptor code feature, as considerably as the m-MiMo parameters aided by AN signal while reducing the transmission power of the AN. The numerical results indicate that the new approach ensures the protection of legitimate users on the channel and minimizes energy expenditure, which potentially gets to this proposed method a greener and secure transmission.

Keywords: 5G, Massive-MiMo, Raptor Codes, Secrecy, Eavesdropping, Artificial Noise, Wiretap Channel

1. Introduction

The technological revolution of the Internet is thriving with the arrival of connected objects. It is expected that by 2020, the mobile cellular network capacity would reach 1000 times that of existing networks [3].

To meet the increasing capacity in these networks, a future technology of wireless networks (5G) is introduced. Based on new approaches and technologies, 5G is considered as a promising wireless system to meet the requirements of the growing data. Similar to all wireless networks, the 5G has a quick and straightforward approach to the channel due to their broadcasting transmission technique. Nevertheless, this characteristic exhibits them to eavesdropping attacks. An eavesdropping attack, as well recognized as a sniffing or snooping attack, an intruder node spies the messages exchanged between users, which heads to the confidentiality issues through the network. This problem is fixed by deploying cryptographic protocols in higher layers of communication systems [4]. Though, due to the dynamic topology of wireless networks, this method suffers from several problems, such as symmetric and asymmetric cryptography key distribution and management, and the high complexity of processing [5].

As a complement solution, the PLS is used for securing the more upper layers.

In 5G wireless communications, the diversity of the promising PLS technologies is the channel coding, m-MiMo, millimeter-wave communications, heterogeneous networks, and other applications such as the non-orthogonal multiple access, full-duplex technology, etc. The m-MiMo is an enhancement of MIMO technology that was recently proposed to secure the physical layer in 5G networks. An example of m-MiMo is presented in Figure 1.

In m-MiMo, hundreds of antennas involve equipping the

base station. This feature allows increasing the capacity by ten times or more and concurrently enhancing the secrecy compared to the traditional MIMO [6].

Furthermore, the large number of antennas permits the transmitter (Alice) to focus perfectly narrow and directional energy in the direction of the legitimate receiver (Bob) and to radiate the AN signal in the direction of any inconsistent intruder which reduces its signal power. Unfortunately, the benefit of secrecy disappears once the eavesdropper (Eve) is equipped with several antennas equal to or more than the number of antennas of the legitimate transmitter. Additionally, the design of AN needed in the m-MiMo usually involves enormous computational complexity, which is inefficient in terms of cost [7]. Moreover, the implementation of AN includes excessive energy which is of the order of $(n)^{\beta}$, n is the noise variance of Bob, $n > 1$, β is a constant > 1. The details of these results are depicted in section 4 of this paper, where we give a theoretical analysis of our proposed approach.

Another mode that can be applied to come up to eavesdropping in the physical layer is the error corrector code approaches. Recently, Raptor codes are employed for their reliability to stop up the transmission between authorized parties. For the sake of understanding, section 3 presents an overview of the Erasure and Rate less to which Raptor code belongs.

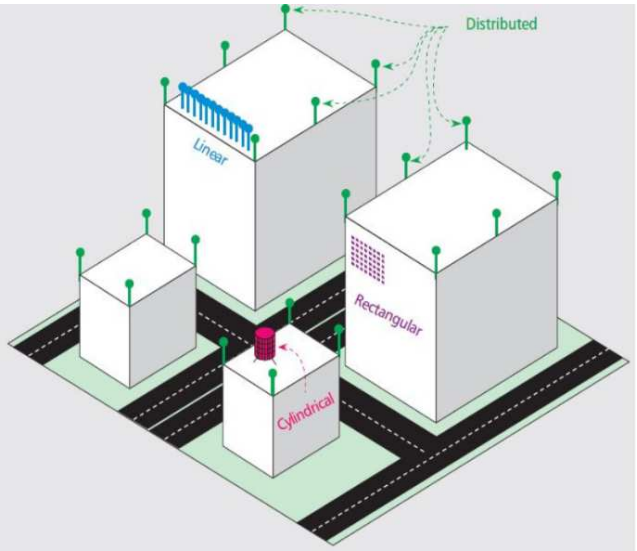

Figure 1. *An example of massive MiMo [6].*

In the Raptor code, which is a class of the fountain code, the transmitter generates on the fly an infinite number of encoded packets. The receivers collect the received bits until they recover the message. Then, they send a STOP message to the source [8]. In the wiretapping channels, this feature can be exploited to secure the physical layer, which implies that the destination must recover the K independent coded packets before the eavesdroppers [9, 10].

Therefore, the signal-to-interference ratio (SNR) of the legitimate receiver must be more significant than that of the intruder to ensure that Bob intercepts the K sufficient packets before Eve at this fourth dimension. Nevertheless, these methods consider an eavesdropper with single antennas. Therefore, these methods cannot be given to the new technologies of 5G wireless networks where the intruder uses them-MiMo, which permits it to have a high SNR to recover the signal quickly. Furthermore, in this case, the Raptor codes can be converted into an appropriate tool for the eavesdropper that can be used to spy on the legitimate channel. Besides, the m-MiMo technology suffers from several limitations, as explained above, that complicate the secrecy management for Raptor code in the presence of an intruder with a large number of antennas. Therefore, to ensure security in wireless channels using Raptor code with a large number of antennas used by eavesdropper, we fully exploit the feature of the Raptor codes where Bob must intercept the K sufficient packets before Eve. In this study, we show that to fill this requirement, the power needed to design AN must be at least ς*(n) instead to that mentioned above, i.e., $(n)^{\beta}$, ς is a constant which is comprised between 1 and β, $1 < \varsigma < \beta$.

Motivated by these observations, we propose to exploit the features of Raptor code taking in count the characteristics of m-MiMo and AN to ensure secrecy while reducing the power consumption to guarantee a secure green transmission. The novelty of our contribution is that it is the first to deal with a security problem in the presence of an intruder using Raptor code and a large number of antennas. Thus, our work is different from other works that treat the secrecy with conventional MiMo. To affirm our statement, we offer a theoretical analysis in this article. In this paper, we did not discuss ergodic capacity (secrecy capacity) because with Fountain code this is not necessary since the transmitted packets of the confidential data are correlated, and only a certain number of packets are required for data recovery [7].

This study can be considered as an extension of two works cited in this paper. The first study belongs to the authors, J. Zhu, and W. Xu, where we add new technologies such as m-MiMo. Furthermore, we studied the Raptor code, which is an application of the fountain code used by the authors [9].

The second extension is done in our previous work; where a theoretical analysis is added to demonstrate how the characteristics of m-MiMo and Raptor code are judiciously exploited to secure the physical layer on wireless networks without using puncturing data [1].

This paper has outlined as follows: Section 2. gives a general review of Erasure and rateless code, the section 3. presents the related work, the section 4 introduces our scheme where we provide a theoretical analysis of our proposed approach, the section 5 presents and discusses the simulation results, and finally, in section 6, we conclude this paper.

2. Erasure and Rate Less Codes

An erasure code is a forward error correction (FEC) code that adds redundancy to the system to correct errors occurred while transmitting data. The source transmits information symbols, adding redundancy to the message, which allows the receiver to retrieve the message without needing to request to retransmit the corrupted packets or acknowledgment to approve received packets. These codes are suitable in the

schemes where retransmissions of the packets are expensive or intolerable.

The Low-Density Parity-Check (LDPC) codes are the essential classes among the erasure codes. Gallager creates them in early 1960. Their decoding is based on iterative belief-propagation (BP) algorithms, which permit them to achieve a decoding performance near to the Shannon boundaries. LDPC codes reach better performance on additive white Gaussian noise (AWGN) channels and generally do not attain the ideal reliability on non-Gaussian channels [11].

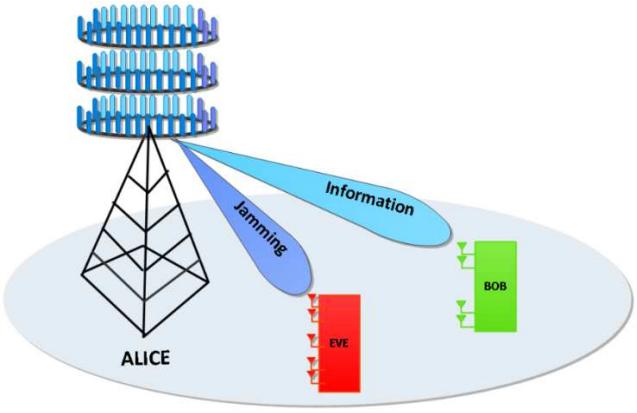

Figure 2. *Wiretap channel [1].*

The emergence of fountain codes makes them a promising code for sparse graph code, namely Luby Transform (LT) and Raptor. The most important application of these codes is the internet or wireless networks [11].

A rateless codes are corrector codes which are categorized by variable rate, and the transmitter generates on the fly an infinite number of encoded packets, the receivers collect the received bits until they recover the message, then they send a STOP message to the source. Fountain code is the code which unifies the proprieties of rate less and erasure codes, and their applications are Luby Transformer LT and Raptor [8].

The codes LT are the first application of universal Fountain codes. Michael Luby designed them in 1998. Its encoding method is based on a bipartite graph which is identical to that used in LDPC codes. Hence its decoding is analogous to that of LDPC. One of their most practical application is a coding technique for distributed multiuser information storage systems [12]. In LT codes, a short augmentation in overhead can be introduced to obtain a performance. The overhead is the variation between the number of the received edges and that of the input edges. A considerable increase in overhead generates an extended decoding latency which leads to an error floor problem because of their processing complexity [13]. To solve the problem of this complexity and to enhance the reliability of LT, Raptor codes are designed in late 2000 by using an additional erasure code [14, 15]. The supplementary erasure code can be an LDPC code [16].

3. Related Work

Several solutions have been proposed in the literature to secure the physical layer from eavesdropping. In this section, we summarize the work that has been done on security using the Fountain codes and those that have used m- MIMOs. The m-MiMo approaches can be classified into two categories. The first category uses m-MiMo aided by AN while the second category uses m-MiMo without the help of AN. In the first category, the bruit signal is generated in the direction of the malicious intruder and the null space channel of the legitimate user, which degrades the intruder's channel without affecting the authorized user. In this context, a solution to secure transmission with AN method over correlated fading channels in multiuser multicell is proposed. For this purpose, the m-MiMo system assisted by maximum ratio transmission (MRT) precoding is used to secure the main channel in the presence of an active eavesdropper which uses multi antennas [17].

A solution for multi-cell setting, when the AN signal cause the inter-cell interference, is considered in system design in the literature [18]. The authors of this proposal introduced a closed-form that derives bounds. The obtained results allow them to predict under what conditions a positive secrecy rate is possible. In the same context of m-MiMo with the AN method, we can find those who focus on optimizing the power allocation between AN and the main channel.

To reduce the complexity of the assignment of the optimal power between the information signal and the AN is considered [19]. The authors of this study recommend a closed formula to reach the confidentiality rate in the declining channels.

Nevertheless, to ensure secrecy, the solutions cited above require that the number of transmitting antennas to be higher than the number of eavesdropper's antennas [20]. Unfortunately, when the intruder uses a large number of antennas for eavesdropping, the secrecy ability would be null, and the secret cannot be guaranteed. Furthermore, the design by AN usually requires immense computational complexity through a null-space calculation when the number of the antennas is large [7].

As an alternative solution, the PLS solutions, that proposed m-MiMo without the aide of AN, is recommended. Those exploits the other physical layer properties to enhance communication security in case of an intruder with a higher number of antennas. One of them, the method proposed to secure the massive MIMO systems via scaling down the power with the increasing number of antennas for both training and information transmission without the help of AN [7]. The authors of this proposition addressed the power efficiency in a pilot-contaminated multi-cell m-MIMO system with the existence of eavesdroppers employing m-MIMO.

T. R. Dean and A. J suggest a physical layer cryptography to secure the channel between Alice and Bob. In their solution, a parallel channel decomposition between Alice and Bob is performed. As the eavesdropper, Eve, has a different channel, it cannot retrieve the signal because of the linear complexity [21]. In the same context, the Original symbol Phase Rotated scheme (OSPR) is proposed in two papers of the literature. This method aims to randomly rotate the phase of the original

symbols at the base station (BS) before they are transmitted. In these papers, the secure communication on the downlink and uplink transmission is considered.

Furthermore, a parameter termed radiated power scaling (RPS) factor is used to optimally correct the overall transmit power with different number of BS antennas in order to reduce power consumption [22, 23]. However, these studies did not consider when Eve uses Raptor codes

Another way to ensure security at the physical layer is the error-correcting code approach. One of these solutions is the punctured LDPC method [24]. In this scheme, the LDPC encoded message is punctured before its transmission. To achieve reliability and secrecy, the authors suppose that the legitimate receiver operates in a high SNR and eavesdropper in low SNR.

Furthermore, it was shown that the puncturing method makes the messages less performant than the messages which are not punctured. Hence, recovering the original word requires high energy to reach the best performance on the legitimate channel. The characteristic of fountain codes of the physical is first studied by H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, where they consider that the quality of the source-destination link is better than that of the eavesdropper link and proposed to adopt a transmit power control (TPC) strategy otherwise [9]. Nevertheless, this method is desirable when the illegitimate receiver is in an outage, and the legitimate receiver has a high SNR.

Another study using the fountain-coding is proposed, later, which is based on an outage prediction, and limited feedback. This method takes into count the real-world systems and the impact of the instantaneous channel state information (CSI) is proposed [10].

However, the studies give a general theoretical analysis of how the fountain code characteristics are exploited to secure the physical layer on wireless networks and did not consider a new wireless network like 5G, which is different because of the use of new technologies such as the m-MiMo. Besides, these studies are not dedicated to a specific category of fountain codes such as Raptor code that performs different from LT.

In our previous work, we propose to use Raptor code based on punctured LDPC to reduce the capacity of intruder channels to recover data [1]. However, the puncturing data need high energy to improve the original message. Furthermore, by using the Fountain code, the transmitted packets of the confidential data are correlated; therefore, only a certain number of packets are required for data recovery [7]. Consequently, in this paper, we consider just Raptor code without punctured LDPC.

Another solution with the fountain code where Raptor codes are used to efficiently forward the information symbols through several parallel paths is recommended [25]. Through their analysis, it has been shown that Raptor codes can be used to guarantee a reliable and robust multiple simultaneous paths. Nevertheless, this work is dedicated to the network layer protection. Besides, the study considers the binary erasure channel which does not consider variation of the channel like the fading and the attenuation of the transmitted signal and additive noise (AWGN) at the receiver. In this paper, certain symbols will be used, as explained below:

Upper case characters in bold indicate matrices $[\cdot]^H$ signify the conjugate of a complex matrix, and $[\cdot]$ † denotes the transposed matrix of the conjugate matrix. The notation E $[\cdot]$ Denotes the mathematical expectation denotes the norm of a vector, and $\| \cdot \|$ denotes the determinant of a matrix. I_M denotes the identity matrix of M*M. Tr(A) is the trace of A. * denotes the multiplication operator.

4. System Model

As represented in Figure 3. Alice wants to transmit an *S* bit message to Bob and uses a Raptor code to encode the *S* bit message. The source block message $S \in \{0,1\}$ of $k \in \{0,1,2\ldots..K\text{-}1\}$ is first encoded with LDPC with a rate R=k/n, where k and n are the length of the data blocks and the codewords respectively. The LDPC codeword is then encoded on LT code to produce the codeword $b_k \in \{0,1\}$ of $k \in \{0,1,2\ldots..K\text{-}1\}$. The code word b_k is modulated in BPSK to generate the symbols vector to an n bit codeword Xn and is sent over an AWGN flat fading channel to Bob.

Eve as passive eavesdropper can move closer to Alice, which allows it to have a stronger received signal to spy the main channel. Suppose that the transmitter, Alice, and the receiver, Bob, are equipped with N_t and N_r antennas, respectively. The intruder Eve has $N_e$antennas to listen to the transmission signal between the transmitter and the receiver $N_e > N_t > N_r$. It is supposed that the channel between the transmitter and the legitimate receiver is known to all parties, but the Channel State Information (CSI) of the intruder channel is not known. An example of a wiretap channel is depicted in Figure 2.

To ensure secrecy, Alice divides the transmit signal into two parts, one that carries the secret message for Bob and the second that gives the AN signal to confuse Eve's channel. Alice determines X as the sum of the data transporting the signal information U and the artificial noise signal.

$$X = U + W \tag{1}$$

U and W are complex Gaussian vectors, W is designed to be in the null space of H, such that

$H*W= 0$

If Z is an orthonormal basis for the null space of H, then:

$W = Z * V$ and $Z * Z^H = I$

H is the channel between Alice and Bob and is a circularly symmetric complex Gaussian random variable with zero mean and variance $\sigma_h^2 = d_{AB}^{-\alpha}$ The coefficients of H are represented by $Nt * Nr$ matrix d_{AB} is the distance between Alice and Bob and α is the path loss coefficient. The received signals at the legitimate and the eavesdropper receivers are determinate respectively as follows:

$$Yb = \mathrm{H}(\mathrm{U} + \mathrm{W}) + \mathrm{n}_b \tag{2}$$

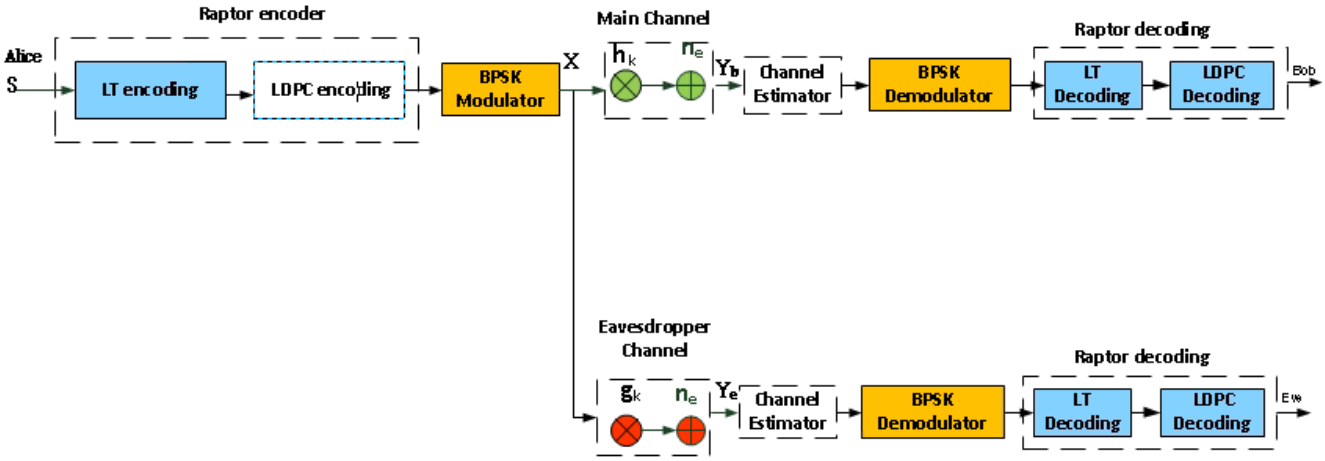

Figure 3. *Diagram Block Model.*

As H*W= 0, the signal Yb of the equation (2) becomes as below

$$Yb = \mathrm{HU} + + \mathrm{n}_b \tag{3}$$

$$Ye = GU + GW + ne \tag{4}$$

n_b, is the Gaussian noise of the receivers, and ne is the Gaussian noise of the intruder, G is the channel between Alice and Eve, and is unknown to the transmitter and the receiver, and G inputs are modeled as independent symmetric Gaussian random variables of mean zero and variance. The coefficients of G are represented by $Nt * Ne$ matrix. The noise signal is supposed to be additive white Gaussian noise (AWGN) is given below:

$$\mathbb{E}\{n_b n_b^H\} = \sigma_b^2$$

$$\mathbb{E}\{n_e n_e^H\} = \sigma_e^2$$

The followed equations give the SNR of Bob and Eve:

$$SNR_b = \frac{H * S * S^H * H^H}{\sigma_b^2}$$

$$SNR_e = \frac{G*S*S^H*G^H}{G*Z*Z^H*G*\sigma_v^2+\sigma_e^2}$$

Since Eve is a passive intruder, it can move closer to Alice, hence $d_{AB}^{\alpha} > d_{AE}^{\alpha}$.

Suppose that Eve and Bob have the same capacity of SISO channel C, let C_e and C_b be the capacity of Eve and Bob respectively in massive MiMo.

Let N_{NS} be the number of antennas in the null space of Bob, $N_{NS} = \dim(\mathrm{Z} = \text{null space (H)})$, The condition to realize the null space is that $N_{NSmin} \leq N_{NS} \leq N_{NSmax}$, where $N_{NSmax} = N_t - One$ and $N_{NSmin} = N_t - N_r$, we suppose that $N_t - N_r > N_r$.

The capacity of Eve can be expressed as follows:

$$C_e = \frac{N_t - N_r}{N_r} * log(I + SNR_b) = (I + SNR_b)^{\beta} \tag{5}$$

$$\Rightarrow I + SNR_e = (I + SNR_b)^{\beta} \tag{6}$$

We suppose $\beta = \frac{N_t - N_r}{N_r} > 1$ As $SNR_b > 0$ and β is a positive integer; we can apply the Binomial theorem to the term $(I + SNR_b)^{\beta}$ which can be written as follow:

$$I + SNR_e = (I + SNR_b)^{\beta} = \sum_{i=0}^{\infty} \binom{\beta}{i} (SNR_b)^{\beta} \tag{7}$$

$$\Rightarrow SNR_e = \sum_{i=1}^{\infty} \binom{\beta}{i} (SNR_b)^{\beta} \tag{8}$$

$\binom{\beta}{i}$ is a binomial coefficient, and can be expressed as follows:

$$\binom{\beta}{i} = \frac{i(i-1)(i-2)(i-\beta+1)}{\beta!}$$

In the worst case, when $\sigma_e \to 0$, the SNR_e is given as follows:

$$SNR_e = \frac{G * S * S^H * G^H}{G * Z * Z^H * G * \sigma_v^2}$$

To ensure the secrecy, it is necessary that $SNR_e < (SNR_b)^{\beta}$, hence

$$\left(\frac{G*S*S^H*G^H}{G*Z*Z^H*G*\sigma_v^2}\right) < \left(\frac{H*S*S^H*H^H}{\sigma_b^2}\right)^{\beta} \tag{9}$$

$$\Rightarrow \sigma_v^2 > (\sigma_b^2)^{-\beta} \tag{10}$$

Suppose that $\sigma_b < 1$, hence, we can write $(\sigma_v)^{\beta} \gg 1$, to achieve the requirement of the equation (9), the transmitter should design AN signal with an energy that is equivalent to $(power\ noise\ of\ Bob)^{\beta}$, which is an enormous energy that makes this method no ecologically secure transmission.

However, by using feature fountain code to secure the channel, this leads to ensuring the inequality below [7, 10]:

$$\varepsilon_{AE} > \varepsilon_{AB} \tag{11}$$

The inequality above (11) allows Bob to intercept the message before Eve does. Since the Raptor code is class and an application of fountain codes, this implies that inequality (10) is also sufficient for raptor codes.

$\varepsilon_{AB}, \varepsilon_{AE}$ Are the outage probabilities at Bob and Eve, respectively, and they are expressed by the equations below [7]:

$$\varepsilon_{AB} = P_r\{(1 + SNR_b) < R\} = 1 - e^{-d_{AB}^{\alpha}/\rho_b} \quad (12)$$

$$\varepsilon_{AE} = P_r\{(1 + SNR_e) < R\} = 1 - e^{-d_{AE}^{\alpha}/\rho_e} \quad (13)$$

$$\rho_b = \frac{P}{\sigma_b}$$

$$\rho_e = \frac{P}{\sigma_v}$$

P is the transmit power. As mentioned above, to ensure the Security it is necessary that $\varepsilon_{AE} > \varepsilon_{AB}$ [7] which means that $\frac{\sigma_v * d_{AE}^{\alpha}}{P} > \frac{\sigma_b * d_{AB}^{\alpha}}{P}$., as $d_{AE}^{\alpha} < d_{AB}^{\alpha}$ this implies that $\sigma_v > \sigma_b$, hence

$$\sigma_v = \varsigma * \sigma_b \quad (14)$$

$\varsigma > 1$ is an integer coefficient.

By comparing the result found in equation (14) with that found of (10), we realize that the power that can be dedicated to design AN using the feature of Raptor code is less than that using massive MiMo aided NA without exploiting a Raptor code feature.

At the receiver, for both Bob and Eve, the Belief Propagation (BP) algorithm is used to achieve the soft decoding process. Figure 4 shows the graph of the encoding and decoding of the Raptor code.

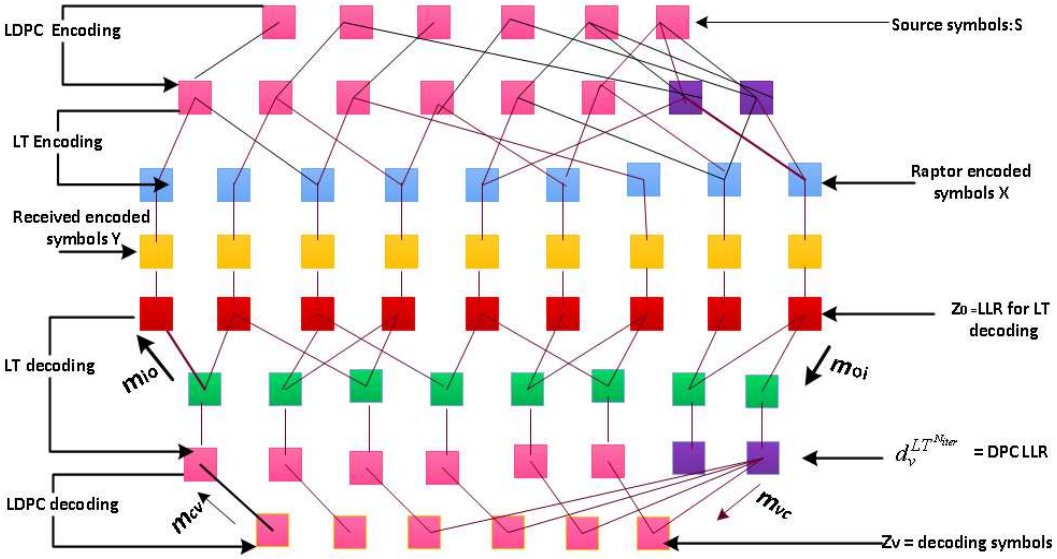

Figure 4. *Raptor encoding and decoding [2].*

The Likelihood Ratios (LLR) of channel for both Bob and Eve are given as follows:

$$Z_{0,b} = \ln\left(\frac{P(\hat{s}_k=1|y_k,h_k)}{P(\hat{s}_k=-1|y_k,h_k)}\right) \quad (15)$$

By employing the independence property between $\hat{S}_k$ and $\hat{h}_k$, and using the Bayes rule, the equation (15) becomes as follows:

$$Z_{0,b} = \ln\left(\frac{P(y_{k|h_k},\hat{s}_k=1)}{P(y_{k|h_k},\hat{s}_k=-1)}\right) + \ln\left(\frac{P(\hat{s}_k=1)}{P(\hat{s}_k=-1)}\right) \quad (16)$$

With equal probability for the input $\hat{S}$, the term on the right side of the equation (16) is equal to zero. In the output of the matched filter, y_k, the probability is given as follows:

$$P(y_{k|h_k}, \hat{s}_k = \pm 1) = \frac{1}{\sigma_b\sqrt{2\pi}} e^{\frac{(y_k \pm h_k)^2}{2\sigma_b^2}} \quad (17)$$

By Substituting (17) in (16), we get

$$Z_{0,b} = \frac{2\hat{h}_k}{\sigma_b^2} Y_b \quad (18)$$

Eve's LLR can be found in the same way as Bob's LLR using the equations (12), (13), (14); hence, it can be expressed as follows:

$$Z_{0,e} = \frac{2\hat{g}_k}{\sigma_v^2} Y_e \quad (19)$$

At the iteration 0 of the BP decoding algorithm, if o and i are neighbors, the received channel LLR from the output node o to the input node i is expressed as follows:

$$m_{o,i}^{(0)} = Z_{0,t} \quad (20)$$

t can take two letters, b or e, to designate Bob or Eve, respectively.

For the following iterations, the LLR updating process of LT decoding is completed as follows:

$$m_{io}^{(l)} = \sum_{o' \neq o} m_{o'i}^{l-1} \quad (21)$$

$$tanh\left(\frac{m_{o,i}^{(l)}}{2}\right) = tanh\left(\frac{z_0}{2}\right) \prod_{i' \neq i} tanh\left(\frac{m_{i',o}^{(l)}}{2}\right) \quad o = 1,\ldots, L \quad (22)$$

$m_{o,i}^{(l)}$ and $m_{io}^{(l)}$ are the messages at iteration l, spent from

the output node o to the input node i and from the input node i to the output node o, respectively. z_0 is the LLR was corresponding to output symbol o calculated in (18), (19), for Bob and Eve respectively, and received from the channel. After processing the decoder for l iterations, the LLR of each input node i is given below

$$d_i^{LT^l} = \sum_{o \in P(i)} m_{oi}^l \tag{23}$$

At iteration N^{itr}, the LLR of the input nodes is calculated, as:

$$d_i^{LT^{Niter}} = \sum_{o \in P(i)} m_{oi}^l \tag{24}$$

Where, $P(i)$, is the sum of overall output bits o adjacent to i. Those LLR, named the output LLR, are the LT decoding LLR, considered as a priori LLR used as an input of the LDPC-decoding.

At iteration 0 of the algorithm, the messages sent by each variable node to its adjacent check nodes are the LLR from the LT decoding. The procedures of the LLR update for decoding LDPC are given by:

$$m_{v,c}^{(0)} = d_v^{LT^{Niter}} \quad \text{if o and i are neighbours} \tag{25}$$

$$tanh\left(\frac{m_{c,v}^{(l)}}{2}\right) = \prod_{\substack{v=1 \\ v' \neq v}}^{n} tanh\left(\frac{m_{v',c}^{(l-1)}}{2}\right) \tag{26}$$

$$m_{vc}^l = m_{v,c}^{(0)} + \sum_{c' \neq c} m_{c',v}^{l-1} \tag{27}$$

m_{vc}^l Moreover, $m_{c,v}^l$ are the messages of the LDPC decoder, they are transferred from the variable nodes v to the check nodes c and from the check nodes c to the variable nodes v, respectively. At the iteration l, at the LDPC decoder, we get:

$$Z_v = \sum m_{c',v}^l \tag{28}$$

For each decoded bit c, v, hard decision is made as follows:

$$\hat{S} = \begin{Bmatrix} 0 \text{ if } Z_v \geq 0 \\ 1 \text{ if } Z_v < 0 \end{Bmatrix} \tag{29}$$

5. Simulation Results

The performance of our scheme is evaluated in this section. The codeword length chosen for LDPC encoding is 80000 bits, the message length is 980 bits, and the code rate is 0.98. The degree of distribution of the LT encoding is the same as that used in and is as follows [2]:

$$\Omega(x) = 0.008x + 049x^2 + 0.166x^3 + 0.073x^4 + 0.083x^5 + 0.056x^8 + 0.037x^9 + 0.056x^{19} + 0.025x^{65} + 0.003x^{66}$$

The number of antennas used by Alice and Bob is 16 and 8, respectively, while Eve uses 32 antennas. The variance of AN is $\sigma_v = Two * \sigma_b$.

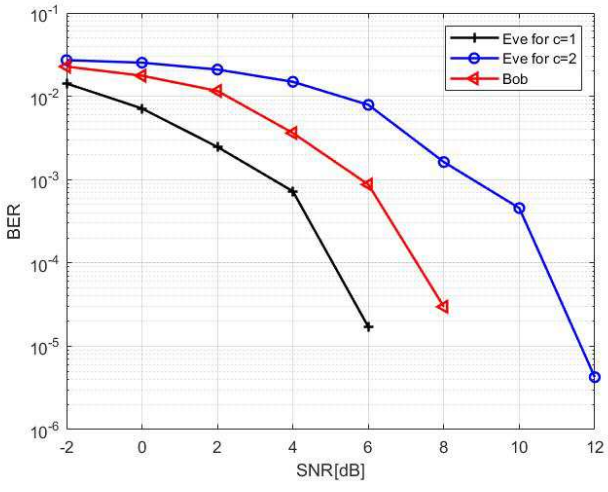

Figure 5. *BER of Bob and Eve.*

Figure 5 shows that when our approach is not applied, Eve can retrieve the information at 6 dB of the SNR threshold before Bob did. However, when the secrecy method is used, Bob is the first to retrieve the message at 8dB of the SNR threshold. As $\sigma_v > \sigma_b$ Eve's performance is reduced concerning that of Bob; therefore, when Bob recovers the message, it sends an acknowledgment of successful decoding to the encoder (Alice) to stop generating the encoded symbols. Since Eve is eavesdropper, it cannot request to retransmit an additional data that allows it to retrieve the message. Hence,

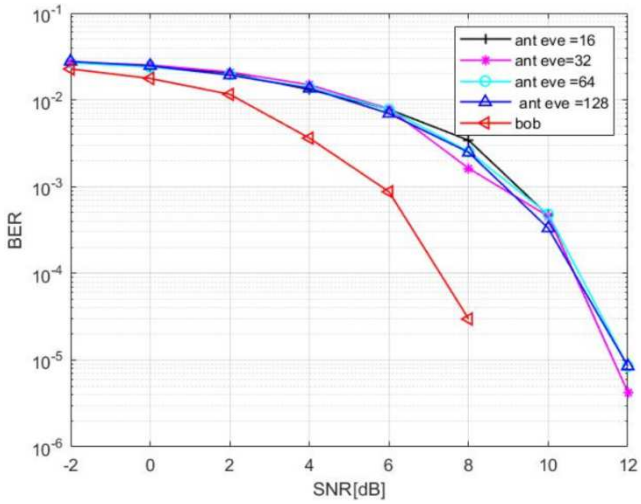

Figure 6. *BER of Eve with different number of antennas.*

Eve is no longer able to recover its signal once Bob succeeds in decoding its message.

Figure 6 shows that despite the number of antennas deployed

by Eve, i.e., 16, 32, 64, 128 antennas, it is unable to recover the data sent by Alice. The graph also shows the possibility of retrieve the channel can happen at SNR threshold value of 12 dB after of Bob's extracting message that of Bob, which allows Bob to be the first to retrieve the message

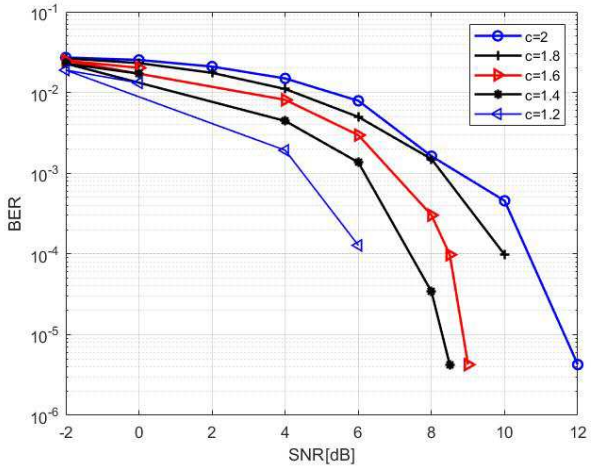

Figure 7. *BER of Eve with different values of coefficient.*

Figure 7 gives an overview of the different values that the coefficient c can take to ensure safety. The graph shows that security is guaranteed for the values of $c > 1.2$, which conforms with equation (14) found in section 5.

The performance of the Raptor code compared to LT and LDPC is also studied. The results are presented in Figure 8. It shows that the Raptor code performs better than the LT and LDPC.

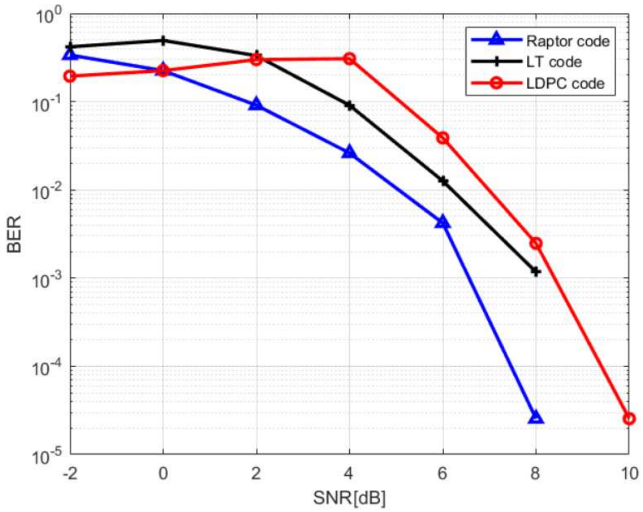

Figure 8. *BER of Bob with LDPC, LT and Raptor codes.*

Since the Raptor code is a succession of tow erasure code, in our case, LDPC and LT, the overhead factor included in LT is studied in this part. The overhead coefficient defines the number of variables that are involved in decoding. In LT codes, when the number of edges is large, a longer processing time is needed to decode the message. The significant amount of edges allows us to recover the message but generates delay and treatment process complexity. Nevertheless, to avoid this inconvenience, Bob must optimally choose the coefficient that will enable it to improve the signal with less delay. Figure 9. Shows that in the low SNR, a more significant number of edges are required to enhance the message. The information can be successfully retrieved at 10dB for the value 2.1 of the overhead coefficient. Though, in lower SNR, it is impossible to recover the message since the BER tends to 0.2 and the overhead factor to 3.

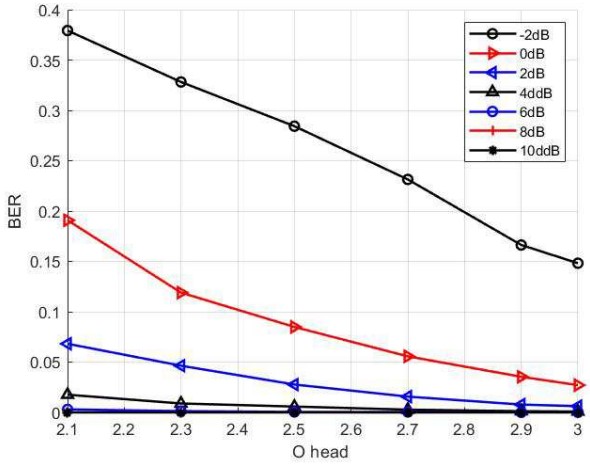

Figure 9. *BER of Bob with different overhead factor.*

6. Conclusion

To address the security problem in m-MiMo for 5G wireless networks, a new approach is proposed in this paper. This approach ensures secrecy against eavesdroppers equipped with a large number of antennas and with high decoding resources. The proposed scheme exploits the features of the m-MiMo technique and Raptor codes to secure the main channel while minimizing the power consumption, which provides a secure green transmission. The question was examined under certain assumptions, such as the supposition of a perfect channel between the transmitter and the legitimate receiver. Analytical expressions for the achievable secrecy of the considered system have been developed to investigate the performance of our proposed scheme.

Numerical results show that our system succeeds in securing the main channel, regardless of the great resources and the large number of antennas used by Eve to spy on Alice. A future work can be realized by considering the Channel State Information (CSI) in the new proposed method.

References

[1] D. Benzid, M. Kadoch, and M. Cheriet, "Raptor Codes based on punctured LDPC for Secrecy in Massive MiMo," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 1884-1889: IEEE.

[2] D. Benzid and M. Kadoch, "Fountain Codes and Linear Filtering to Mitigate Pilot Contamination Issue in Massive MiMo," *Network and Communication Technologies,* vol. 4, p. 1, 01/10 2019.

[3] Y. Zhou, L. Liu, H. Du, L. Tian, X. Wang, and J. Shi, "An overview on intercell interference management in mobile cellular networks: From 2G to 5G," in *2014 IEEE International Conference on Communication Systems*, 2014, pp. 217-221: IEEE.

[4] Y. Zhu, Y. Zhou, S. Patel, X. Chen, L. Pang, and Z. Xue, "Artificial noise generated in MIMO scenario: Optimal power design," *IEEE Signal Processing Letters,* vol. 20, no. 10, pp. 964-967, 2013.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 16, no. 3, pp. 1550-1573, 2014.

[6] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next-generation wireless systems," *IEEE communications magazine,* vol. 52, no. 2, pp. 186-195, 2014.

[7] J. Zhu and W. Xu, "Securing massive MIMO via power scaling," *IEEE Communications Letters,* vol. 20, no. 5, pp. 1014-1017, 2016.

[8] D. J. MacKay, "Fountain codes," 2004.

[9] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting Fountain codes for secure wireless delivery," *IEEE Communications Letters,* vol. 18, no. 5, pp. 777-780, 2014.

[10] L. Sun and H. Xu, "Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback," *IEEE Transactions on Vehicular Technology,* vol. 68, no. 1, pp. 740-753, 2019.

[11] P. Farrell and B. Honary, "Capacity approaching codes design and implementation," *IEE Proceedings-Communications,* vol. 152, no. 6, pp. 1060-1061, 2005.

[12] P. G. F. Jorge Castiñeira Moreira, *ESSENTIALS OF ERROR-CONTROL CODING*. John Wiley & Sons Ltd, 2006.

[13] X. Yuan and L. Ping, "On systematic LT codes," *IEEE Communications letters,* vol. 12, no. 9, pp. 681-683, 2008.

[14] A. Shokrollahi and M. Luby, "Raptor codes," *Foundations and trends® in communications and information theory,* vol. 6, no. 3–4, pp. 213-322, 2011.

[15] T. Stockhammer, A. Shokrollahi, M. Watson, M. Luby, and T. Gasiba, "Application layer forward error correction for mobile multimedia broadcasting," *Handbook of mobile broadcasting: DVB-H, DMB, ISDB-T and media flo,* pp. 239-280, 2008.

[16] W. Ryan and S. Lin, *Channel codes: classical and modern*. Cambridge university press, 2009.

[17] H. Wei, D. Wang, X. Hou, Y. Zhu, and J. Zhu, "Secrecy analysis for massive MIMO systems with internal eavesdroppers," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1-5: IEEE.

[18] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications,* vol. 13, no. 9, pp. 4766-4781, 2014.

[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology,* vol. 59, no. 8, pp. 3831-3842, 2010.

[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications,* vol. 7, no. 6, 2008.

[21] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive MIMO," *IEEE Transactions on Information Theory,* vol. 63, no. 8, pp. 5419-5436, 2017.

[22] B. Chen *et al.*, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access,* vol. 4, pp. 5374-5384, 2016.

[23] B. Chen, C. Zhu, W. Li, J. Wei, V. C. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access,* vol. 4, pp. 3016-3025, 2016.

[24] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Transactions on Information Forensics and Security,* vol. 6, no. 3, pp. 532-540, 2011.

[25] A. Kacewicz and S. B. Wicker, "Secrecy and reliability using Raptor codes in the presence of a wiretapper in a multiple path wireless network," in *2009 International Conference on Wireless Communications & Signal Processing*, 2009, pp. 1-5.

[26] O. Etesami and A. Shokrollahi, "Raptor codes on binary memoryless symmetric channels," *IEEE Transactions on Information Theory,* vol. 52, no. 5, pp. 2033-2051, 2006.