Physical Layer Security in 5G networks using Artificial Noise Precoding

P. Chandra Sekhar
Research Scholar,
JNTU-Kakinada,
Assistant Professor
Dept of ECE, CBIT(A),
Hyderabad

T. S. N. Murthy
Assistant Professor
Dept of ECE
JNTU-GV College of Engineering(A),
Vizianagaram,
Andhra Pradesh

Abstract: - Fifth Generation (5G) wireless communication networks are becoming more and more predominant in every aspect of society, which raises serious security concerns. These days, maintaining confidentiality, privacy, integrity, and information security are all crucial issues. In wireless transmission, noise and interference are traditionally regarded as disastrous necessities. Furthermore, it has been revealed that detected interference helps the receiving end predict signals. Furthermore, traditional reasonable secrecy coding schemes have somewhat low security rates to ensure the security required for 5G communications. Therefore, using a precoding method based on artificial noise (AN), the concepts of massive Multiple-Input-Multiple-Output (MIMO) and Non-Orthogonal Multiple Access (NOMA) are integrated for the physical layer security of 5G wireless communication networks. The RSMO methodology serves as the basis for the modification of the precoding process. The performance with respect to power, secrecy rate, Bit Error Rate is observed.

Keywords: Physical layer security, AN-based precoding, Rider Optimization Algorithm, Spider Monkey Optimization, Physical layer security.

1. Introduction

More people are worried about the safety of wireless communication, now that Fifth Generation (5G) wireless communication is used in more areas of life. Cryptography methods can be used at a higher level to provide security, or PLS can be used at the physical level [1]. When it comes to 5G networks, using PLS instead of cryptography has two levels of benefits. First, PLS don't depend on how hard the calculations are [2]. This means that a secure link can be made even if eav has powerful equipment. On the other hand, cryptography methods aren't completely secure if someone with enough computing power can listen in [3]. So that 5G networks can meet all of their different service needs, the devices are linked to hubs with varying amounts of power and computing power. Second, because 5G networks are decentralised [4], the nodes can join or leave the system at any time for no given reason. In this case, it is hard to keep track of and share cryptography keys. Because of this, PLS methods are used to send data securely or to make and share cryptography keys [5]. Physical Layer Security (PLS) was looked into as a good way to make sure that wireless interactions are safe by incorporating channel characteristics [6]. There are two main types of PLS methods: the first creates a secret key from the channel [7], and the second uses the inherent randomness of channels that don't have a secret key to make safe transmission models. The second type is getting a lot of attention, and more studies have been done on it [8,9]. PLS also uses different things, like fade and noise, to make sure security [9,10].

5G technologies, including NOMA, millimetre wave, and massive MIMO, are being implemented to address security concerns posed by eavesdroppers who continually attempt to disrupt data transmission [6]. mMIMO is examined as a crucial enabling technology for 5G

wireless standards [5]. The extensive antenna arrays are employed for persistent spatial multiplexing and primarily focus radiated energy towards specific spatial directions in mMIMO systems [11,12]. Consequently, mMIMO offers unmatched improvements in energy and spectrum efficiencies when compared to conventional MIMO. MIMO systems typically utilise linear precoding techniques, which provide significant enhancements in power, bandwidth, and energy efficiency compared to traditional multiuser MIMO systems [13,14].

Multiple access strategies serve as catalysts in mobile networks, with orthogonal multiple access (OMA) being the predominant access technology. The number of subscribers that a system may support is contingent upon the availability of orthogonal resources. Furthermore, the synchronisation, which constitutes a system need, is significantly insufficient to ensure the orthogonality of resource allocation for users. Consequently, OMA finds it challenging to fulfil the data rate needs of the 5G network. A new multi-access strategy known as non-orthogonal multiple access (NOMA) was introduced to address the limitations of 5G technology [15, 16]. NOMA is regarded as an advanced technology in 5G networks due to its superior spectral efficiency [17]. Furthermore, it is indicated that NOMA can integrate with the existing Multiple Access (MA) framework as it employs power multiplexing. The performance of the downlink NOMA model with randomly selected users was examined in [5]. The mutual synchronised wireless power transfer-enabled NOMA system was created in [18], wherein a NOMA user benefiting from favourable channel conditions serves as an energy harvesting resource to assist a NOMA user affected by poor channel conditions [19]. The study in [12] addressed a power allocation optimisation problem for heterogeneous users, focussing on user fairness within a NOMA system.

Wyner introduced the wiretap channel for point-to-point communication, which was subsequently extended by Csiszár and Körner to encompass broadcast channels [20]. If the receiver experiences superior channel conditions relative to the eavesdropper, a positive security capacity is attained [21]. To provide secure communication despite the eavesdropper's channel conditions being superior to the receiver's, numerous strategies have been proposed. [22] Employing AN or a recognised interference to obfuscate the eavesdropper is one technique to enhance security. The level of secrecy can be enhanced when the transmitter is aided by an interfering source that transmits random codewords at a rate allowing the receiver to decode them, while remaining unintelligible to the eavesdropper [23]. MIMO systems can broadcast information and generated noise concurrently to provide security in faded channels [24].

Aditya and Pooja developed a precoding approach for massive MIMO and NOMA based PLS. This solution involves a pre-coder created primarily based on the characteristics of massive MIMO architecture. The performance was significantly improved across all Signal to Noise Ratio (SNR) values [9, 1-4]. Hui-Ming Wang et al. [10] proposed an access threshold-enabled secrecy mobile association technique for physical layer security in a heterogeneous cellular network. This approach associates each user with the base station by providing the highest trimmed average received signal. An accurate integral representation of analytically manageable expressions and connection probabilities was developed. This approach significantly enhanced the performance of secrecy throughput. Huiqing Bai et al. [12] presented an AN-assisted polar coding method for physical layer security. A security coding method-based artificial noise (AN) was devised, utilising the secret bits from the last transmission code block as AN. A suboptimal jamming position selection model was then created to enhance the Bit Error Rate (BER) for the eavesdropper. This model achieved a superior secrecy rate. Muhammad R. A. Khandaker et al. [25] developed an artificial neural network-assisted secure precoding technique for physical layer security. The AN type, initially

built for the intended receiver, utilised constructive interference. A secure precoding approach was then developed utilising eavesdroppers' CSI statistics to reduce essential transmission power. This model achieved significant performance improvement, while essential confidentiality measures against eavesdropping were not taken into account for enhanced system efficacy.

Hayder Al-Hraishawiet al. [26] proposed a secure communication method for a cognitive multi-user mMIMO network utilizing spectrum sharing. The PLS approach was designed for both primary and secondary transmission via AN generation and zero-forcing precoders. Specifically, precoders were created utilizing the channel estimates affected by pilot contamination. The model indicates that PLS communication was established for the primary and secondary mMIMO configurations with channel-phase pilot contamination. Zhijin Qin et al. [27] developed PLS utilizing NOMA in large-scale networks. Precise and asymptotic expressions for security outage probability were derived to evaluate security performance. The performance of NOMA networks was improved by expanding the boundaries of the limited region. Jun Zhu et al. [28] developed polynomial data and AN pre-coders that closely simulate a secure massive MIMO system. Linear precoding of data and artificial noise were utilized to enhance secrecy. This method significantly improved the SINR performance in comparison to a random pre-coder. Yanjun Chen et al. [29] introduced artificial neural network-based physical layer security in cellular networks. Furthermore, an AN-based transmission method was implemented in BS for secure communication. This approach markedly improved the confidentiality performance of the cellular link.

Commonly utilized precoding techniques for the security of mMIMO are presented in [30]. The precoding method was also executed based on AN. Additionally, AN is produced to undermine the efficacy of eav. However, it does not affect genuine user performance. The application of artificial noise (AN) for secure massive MIMO architecture is detailed in references [31, 32], where AN precoding is utilized to ensure confidentiality. The confidentiality feature is refined according to AN to improve system performance [33].

The organization of the remaining paper sections is as follows: Section 2 explains the literature review of current physical layer security techniques in 5G networks and the challenges these techniques face. Section 3 presents a model of the large MIMO-NOMA structure system. Section 4 discusses the developed RSMO technique. Section 5 presents the results and discussion of the suggested RSMO model, while Section 6 concludes the paper.

2. Motivation

The challenges experienced by existing traditional physical layer security in a 5G network approaches are considered as motivation for developing new physical layer security model in 5G network.

2.1 Literature survey

This section presents a literature review of various existing physical layer security techniques in 5G networks. Aditya Trivedi and Pooja Singh developed a precoding approach for NOMA and mMIMO-based PLS. This strategy involves the building of a pre-coder, which primarily relies on the characteristics of massive MIMO architecture. The performance was significantly improved for all Signal to Noise Ratio (SNR) values. Hui-Ming Wang et al. [5] proposed an access threshold-enabled secrecy mobile association technique for enhancing physical layer

security in a heterogeneous cellular network. This approach associates each user with the base station by providing the highest trimmed average received signal. A precise integral representation of an analytically tractable expression and connection probability was developed. This technique significantly enhanced secrecy throughput performance. Huiqing Bai et al. [6] presented an artificial neural network-assisted polar coding method for physical layer security. A security coding method-based artificial noise (AN) was devised, utilising the secret bits from the last transmission code block as AN. A suboptimal jamming position selection model was then created to enhance the Bit Error Rate (BER) of the eavesdropper. This model achieved a superior secrecy rate, while additional iterations were necessary in this technique to improve system efficiency. Muhammad R. A. Khandaker et al. [7] developed an artificial neural network-assisted secure precoding technique for physical layer security. The AN type was initially created for the intended receiver using constructive interference. A secure precoding approach was then developed utilising eavesdroppers' CSI statistics to reduce essential transmission power. This model achieved significant performance improvement, while essential confidentiality measures against eavesdropping were not taken into account for enhanced system performance.

Hayder Al-Hraishawi et al. [8] proposed a secure communication method for a cognitive multi-user massive MIMO network utilising spectrum sharing. The physical layer security technique was established for secondary and primary transmission via artificial noise generation and zero-forcing precoders. Specifically, pre-coders were produced utilising channel estimates affected by pilot contamination. The model reveals that secure communication at the physical layer was established for the primary and secondary massive MIMO configurations, considering channel phase pilot contamination. Nonetheless, the calculation of null space-enabled pre-coders proved to be exceedingly challenging. Zhijin Qin et al. [9] developed physical layer security by the utilisation of NOMA in large-scale networks. Precise and asymptotic expressions for security outage probability were developed for evaluating security performance. The performance of NOMA networks improved by expanding the confines of the designated area. This strategy inadvertently allows eavesdroppers, hence compromising secrecy performance. Jun Zhu et al. [10] developed polynomial data and AN pre-coders that closely emulate a secure massive MIMO system. Linear precoding of data and artificial noise were employed to enhance concealment. This strategy significantly improved SINR performance compared to random precoding; however, this model lacks a sufficient security mechanism to properly mitigate eavesdropper channels. Yanjun Chen et al. [11] introduced artificial neural network-based physical layer security in cellular networks. Furthermore, an AN-based transmission method was implemented in BS for secure communication. This method markedly improved the secrecy performance of the cellular link; nevertheless, it did not succeed in enhancing the dependable communication of standard Device-to-Device (D2D) links.

3. System model

Let's assume that the relay-based massive MIMO NOMA system consists of B antennas for the base station (BS) and R antennas for the amplify and forward (AF) relay, with B being larger than R. Additionally, each user pair is equipped with a single antenna. Furthermore, assuming two single-antenna users as a NOMA pair—one strong user (SU2) and one poor user (PU1)—let's classify them according to the channel characteristics in the availability of an eavesdropper with multiple antennas (UE). Additionally, eavesdroppers have the ability to intercept messages sent by massive MIMO BS and relay them to users. The AF relay amplifies the received signal before sending it to users. Each channel has both minute-scale self-regulating Rayleigh fading and large-scale route loss. The large MIMO base station uses precoding

techniques to send the signal to the relay during the first time interval. The relay relays the received signal to the users via the second instance interval. We indicate both the relay-to-user channel matrix gain (H) and the massive MIMO BS-to-relay channel matrix gain (T). Typically, we cascade massive MIMO BS to user channels. The symbols K and L represent the massive MIMO BS to the eavesdropper, and the relay represents the eavesdropper channel matrix gain. Figure 1 shows the huge MIMO NOMA structure system model[4].

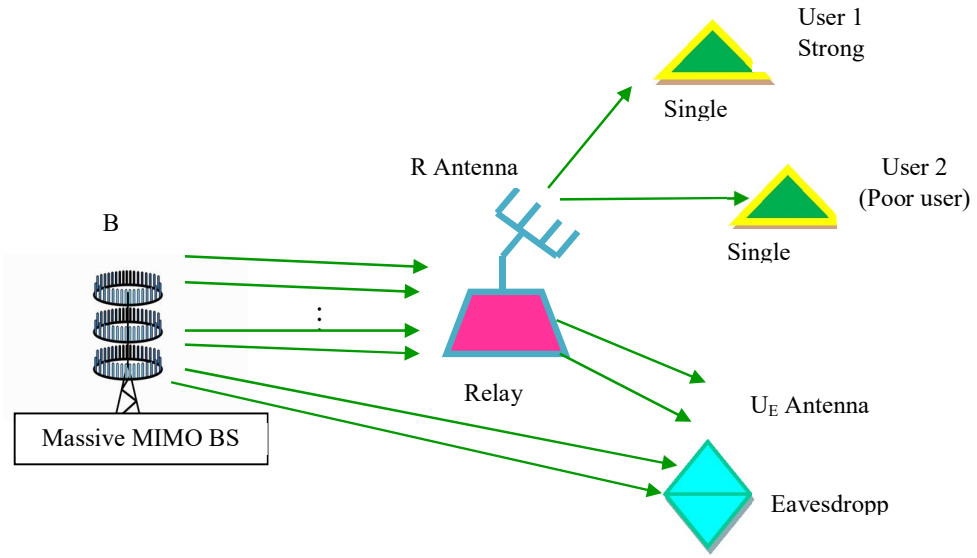

Figure 1. System model of massive MIMO-NOMA system

Here, every channel is designed in uniform model, and it is specified as follows [28],

3.1 Accession of Channel State Information

The fundamental need for Successive Interference Cancellation (SIC) is inclusion ideal Channel State Information (CSI) in NOMA model. Due to the large number of BS antennas in the massive MIMO construction, it is not possible to evaluate the downlink channel at the user node. Hence estimated at MMBS and relay using pilot signalling. Minimum Mean Square Error (MMSE) estimators are specified as follows [25].

$$\hat{T} = Q_T(Q_T D_{e1} + E_R)^{-1}(T\sqrt{D_{e1}} + U_T)\sqrt{D_{e1}} \quad (2)$$

$$\hat{H} = Q_H(Q_H D_{e2} + E_S)^{-1}(H\sqrt{D_{e1}} + U_H)\sqrt{D_{e2}} \quad (3)$$

3.2 Signal model

In first time interval, massive MIMO BS transmits the signal vector as,

$$d_b = D_{bf} * g_b * \hat{G} \quad (3)$$

where,

$$g_b = \beta_{11} P_1 + \beta_{22} P_2 \quad (4)$$

where, β_{11} and β_{22} are power allocation elements for two users, which satisfies $\beta_{11}{}^2 + \beta_{22}{}^2 = 1$.

The signal received at relay by Massive MIMO BS is illustrated as,

$$d_p = T * d_b + U_B \tag{5}$$

where, T denotes channel matrix gain from massive MIMO BS to relay.

The broadcast signal from huge MIMO BS is likewise intended to be leaked to an eavesdropper. The received signal at eavesdropper by massive MIMO BS is referred as,

$$d_j = F * d_b + U_E \tag{6}$$

4. Proposed physical layer security in 5G networks

This section delineates the established PLS in the 5G utilising an AN-based precoding scheme. The secrecy rates of conventional realistic secrecy coding methods are relatively low to meet the security requirements of 5G communications. Consequently, mMIMO and NOMA principles are integrated into the physical layer security of 5G wireless communication networks using an AN-based precoding architecture. The RSMO model taken from [4].

4.1 Pre-coding using AN

The signal transmitted from MMBS in first interval through engaging AN precoding theory, which is specified by,

$$d_{bAN} = D_b * g_b * \hat{G} + D_{AN} UO v_{AN} \tag{7}$$

where, D_{AN} refers power allocated to AN signal at massive MIMO BS, v_{AN} indicates AN vector and UO depicts precoding AN matrix. Equations (1) to (6) will accordingly [4].

4.2 Rider spider monkey optimization-based precoding AN Matrix

The optimal development of a pre-coding AN matrix is performed here using the established RSMO technique [4].

4.2.1 Fitness function

To find the optimum option for the pre-coding AN matrix's optimal generation, the fitness measure is calculated. Here, user and eavesdropper capacities are taken into account when estimating the fitness function, which is stated as,

$$F = \left\lceil B_{p,j} - B_{E,t} \right\rceil^+ \tag{8}$$

where, $\lceil \ \rceil^+ = \max(x,0)$, $B_{p,j}$ indicates users' capacity, and $B_{E,t}$ represents eavesdropper capacity.

5. Results and discussion

The results of the developed RSMO approach for the best pre-coding AN matrix creation is revealed in this part. The following is a list of the comparison methodologies, comparative analysis, comparative discussion, database description, and experimental setup and performance matrix is taken from [4].

5.3 Comparative techniques

The performance of developed RSMO model is compared with traditional techniques, such as AN precoding [1], truncated ARSP [2], AN-aided polar coding method [3] and secure communication model [5].

5.4 Comparative analysis

Comparative examination of the RSMO approach with respect to antenna size 16×16, 32×32 and 64×64 by varying Signal to Noise Ratio (SNR) in terms of power, security rate and BER is discussed in this section.

5.4.1 Comparison for antenna size 16×16

Figure 4 illustrates the comparative analysis of the developed RSMO method about antenna size, focussing on BER, power, and security rate. Figure 4 a) illustrates the comparative examination of Bit Error Rate (BER) across different Signal-to-Noise Ratio (SNR) values. The Bit Error Rate (BER) of the new RSMO model is 0.003105, whereas previous approaches exhibit the following BERs: AN precoding at 0.463424, truncated ARSP at 0.009762, AN-aided polar coding at 0.008532, and the secure communication model at 0.003146, all measured at a Signal-to-Noise Ratio (SNR) of 10 dB. Figure 4 b) illustrates the comparative examination of power as a function of changing SNR values. At an SNR of 10 dB, the power achieved by AN precoding, shortened ARSP, AN-aided polar coding method, and the created RSMO algorithm are 0.2183 Watts, 0.2352 Watts, 0.224 Watts, 0.2472 Watts, and 0.243 Watts, respectively. Figure 4 b) presents a comparative analysis of the security rate across various SNR values. The security rate of the created RSMO methodology is 0.6807, while existing approaches such as AN precoding, truncated ARSP, AN-aided polar coding, and secure communication approach have security rates of 0.6100, 0.5872, 0.6233, and 0.6549, respectively, at 10 dB SNR. The developed RSMO technique demonstrates performance enhancements of 14.97%, 10.89%, 10.30%, and 3.90% relative to conventional techniques.

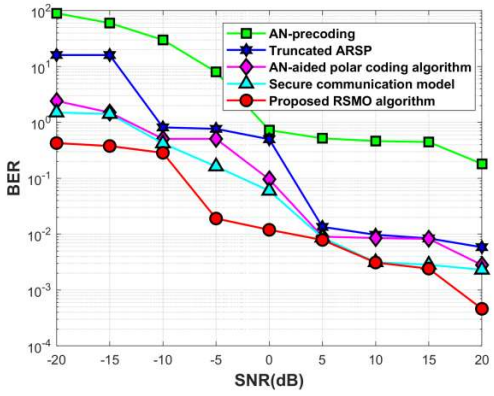

Figure 4A. BER vs SNR with antenna size 16×16

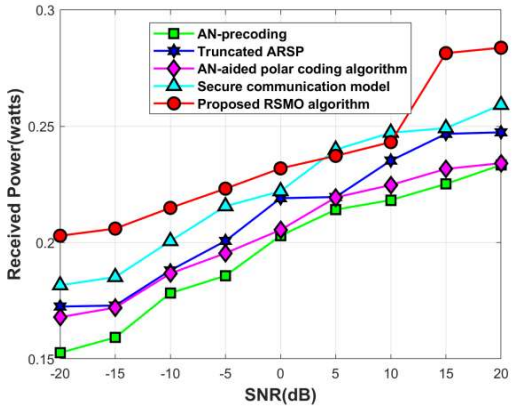

Figure 4B. Received power vs SNR with antenna size 16×16

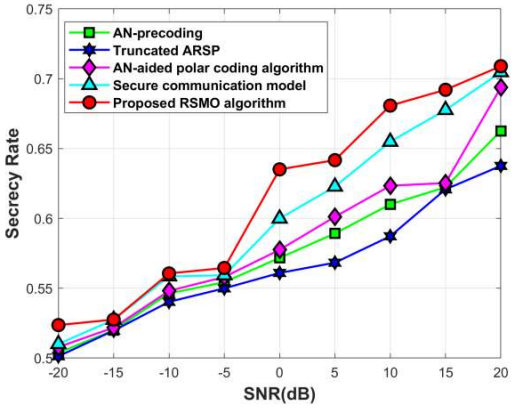

Figure 4C. Secrecy rate vs SNR with antenna size 16×16

5.4.2 Comparison for antenna size 32×32

Figure 5 illustrates the comparative study of the created RSMO method concerning antenna size in terms of Bit Error Rate (BER), power, and security rate. Figure 5 a) illustrates the comparative examination of Bit Error Rate (BER) across different Signal-to-Noise Ratios (SNR). The Bit Error Rate (BER) of the proposed RSMO model is 0.00295, whereas the BERs of existing approaches are as follows: AN precoding is 0.4595, truncated ARSP is 0.01445, AN-aided polar coding method is 0.005412, and the secure communication model is 0.00388, all at a Signal-to-Noise Ratio (SNR) of 10 dB. Figure 5 b) presents a comparative examination of power as a function of varied SNR values. At an SNR of 10 dB, the power achieved by AN precoding, shortened ARSP, AN-aided polar coding method, and the created RSMO algorithm are 0.25528 Watts, 0.2457 Watts, 0.2562 Watts, 0.2755 Watts, and 0.32538 Watts, respectively. Figure 5 b) presents a comparative analysis of the security rate across various SNR values. The security rate of the created RSMO methodology is 0.7219, while existing approaches such as AN precoding, truncated ARSP, AN-aided polar coding, and secure communication approach have rates of 0.633897, 0.6530, 0.6573, and 0.6639, respectively, at 10 dB SNR. The performance enhancements of the new RSMO methodology are 7.81%, 6.72%, 4.22%, and 9.66% in comparison to conventional methods.

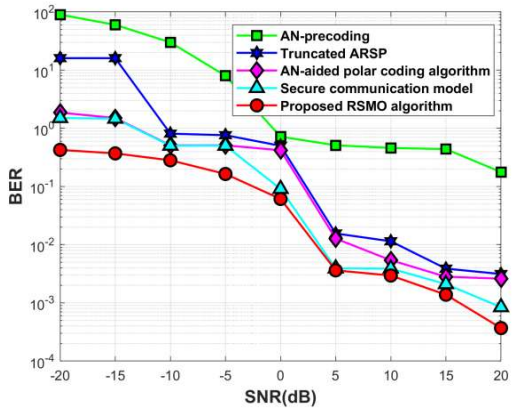

Figure 5A. BER vs SNR with antenna size 32x32

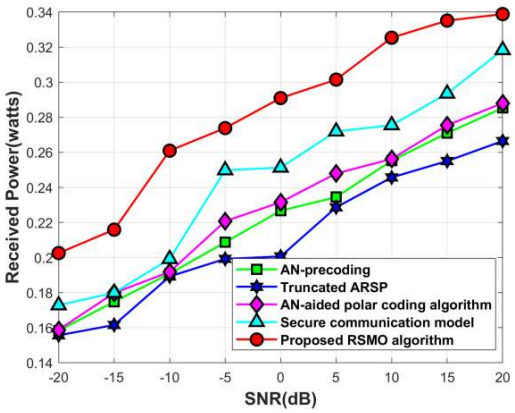

Figure 5B. Received power vs SNR with antenna size 32x32

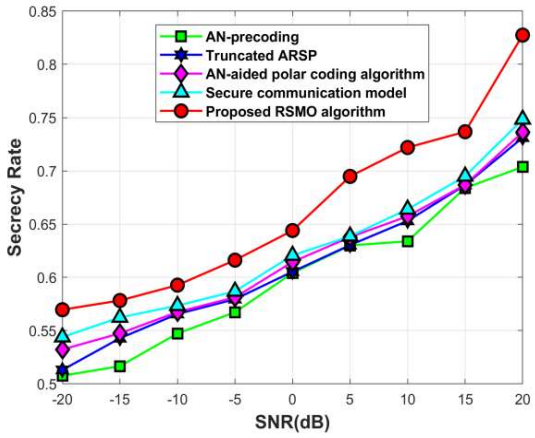

Figure 5C. Security rate vs SNR with antenna size 32x32

5.4.3 Comparison for antenna size 64×64

Figure 6 illustrates the comparative study of the created RSMO method about antenna size in terms of Bit Error Rate (BER), power, and security rate. Figure 6 a) illustrates the comparative examination of Bit Error Rate (BER) across different Signal-to-Noise Ratio (SNR) values. The Bit Error Rate (BER) of the new RSMO model is 0.00173, whereas existing approaches exhibit the following BERs: AN precoding at 0.207103, truncated ARSP at 0.010222, AN-aided polar coding at 0.00307, and the secure communication model at 0.002001, all measured at a Signal-to-Noise Ratio (SNR) of 10 dB. Figure 6 b) illustrates the comparative examination of power as a function of changing SNR values. At an SNR of 10 dB, the power achieved by AN precoding, shortened ARSP, AN-aided polar coding method, and the created RSMO algorithm are 0.2901 Watts, 0.2886 Watts, 0.3046 Watts, 0.3078 Watts, and 0.3291 Watts, respectively. Figure 6 b) presents a comparative analysis of the security rate across various SNR values. The security rate of the new RSMO methodology is 0.78104, whereas existing approaches such as AN precoding, truncated ARSP, AN-aided polar coding, and secure communication approach have security rates of 0.6948, 0.6634, 0.7024, and 0.7531, respectively, at 10 dB SNR. Moreover, the performance enhancements of the created RSMO technique are 15.49%, 7.74%, 12.82%, and 5.78% in comparison to conventional procedures.

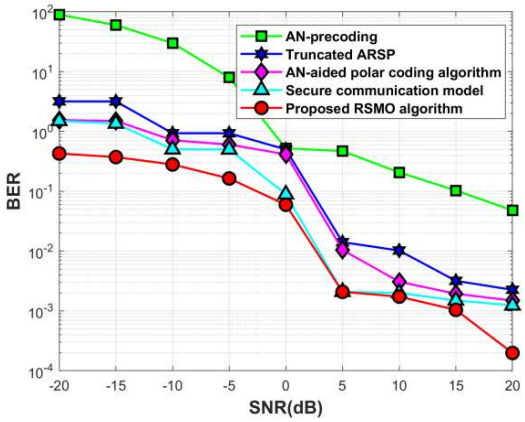

Figure 6A. BER vs SNR with antenna size 64×64 .

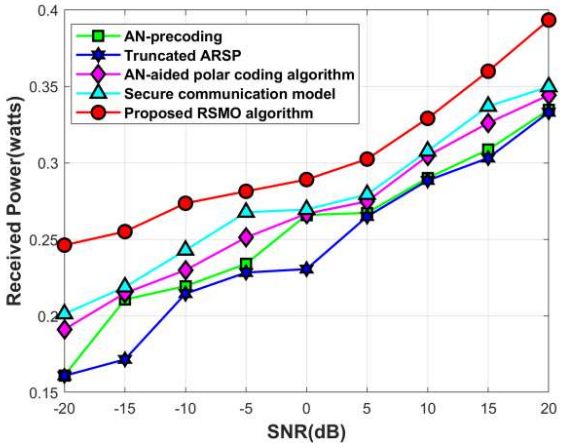

Figure 6B. Received power vs SNR with antenna size 64x64

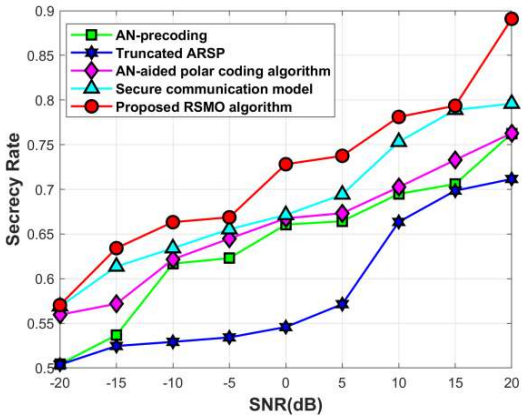

Figure 6C. Security rate vs SNR 64×64

5.5 Comparative discussion:

Table 2 illustrates the comparative analysis of the created RSMO approach with various antenna sizes about BER, power, and security rate when SNR is varied. The Bit Error Rate (BER) for AN pre-coding is 0.04778, for Truncated ARSP is 0.00225, for the AN-aided polar coding technique is 0.001487, for the secure communication system is 0.001236, and for the designed RSMO algorithm is 0.000198, with a Signal-to-Noise Ratio (SNR) of 20 dB. Furthermore, the power output achieved by the created RSMO approach is 0.39345 Watts, while the power values for AN pre-coding, Truncated ARSP, AN-aided polar coding method, and Secure communication procedure are 0.33474 Watts, 0.33311 Watts, 0.344334 Watts, and 0.34984 Watts, respectively, at a 20 dB SNR. At an SNR of 20 dB, the security rates are as follows: AN pre-coding yields 0.762532, Truncated ARSP results in 0.711568, the AN-aided polar coding algorithm achieves 0.76286, the Secure communication system provides 0.79590, and the created RSMO algorithm attains 0.890885. Consequently, the comparative table clearly indicates that the suggested strategy achieved enhanced performance with a power of 0.39345 Watts, with a Bit Error Rate (BER) of 0.000198 and a security rate of 0.890885.

Table 2. Comparative discussion

Antenna Dimensions	Metrics	AN pre-coding	Truncated ARSP	AN-aided polar coding algorithm	Secure communication model	Proposed RSMO algorithm
16×16	**BER**	0.181612	0.005843	0.002809	0.002306	0.000461
	Power (Watts)	0.23338	0.247417	0.23416	0.2592	0.28376
	Security rate	0.66267	0.63763	0.69374	0.7047	0.70900
32×32	**BER**	0.176911	0.003133	0.002606	0.000844	0.000369
	Power (Watts)	0.28530	0.266482	0.288059	0.318369	0.338846

	Security rate	0.70376	0.731151	0.736356	0.748387	0.82747
64×64	**BER**	0.04778	0.00225	0.001487	0.001236	**0.000198**
	Power (Watts)	0.33474	0.33311	0.344334	0.34984	**0.39345**
	Security rate	0.762532	0.711568	0.76286	0.79590	**0.890885**

5.6 Analysis based on computational time

Table 2 shows the analysis based on computation methods for proposed methods. Comparing to the existing methods the proposed RSMO algorithm obtains less computation time of 5.12s.

Table: 2 computation time

Metrics	**AN pre-coding**	**Truncated ARSP**	**AN-aided polar coding algorithm**	**Secure communication model**	**Proposed RSMO algorithm**
Computation time	9.87s	8.36s	7.05s	6.92s	5.12s

6. Conclusion

This research introduces an artificial neural network-based precoding solution for enhancing physical layer security in 5G networks. Typically, noise and interference are regarded as detrimental elements in wireless network transmission. The secrecy rate of current realistic secrecy coding methods is insufficient to meet the security requirements of 5G networks. Consequently, massive MIMO and NOMA theories are integrated for the physical layer security of the 5G wireless communication network using an AN-based precoding model. The MIMO-NOMA structure is simulated, and initial data symbols are transferred while ensuring a guaranteed secrecy rate. This model modifies the precoding procedures utilised in [1] by employing the proposed RSMO methodology to minimise the MMSE objective function. The newly created RSMO algorithm integrates the SMO model and ROA. The security of the physical layer in 5G networks is guaranteed by an optimum AN-based precoding technique. Furthermore, the received data symbol undergoes MMSE-based equalisation, de-interleaving, and decoding at the receiver end. The efficacy of the developed RSMO algorithm is assessed using three performance metrics: Bit Error Rate (BER) of 0.000198, power consumption of 39345 Watts, and a security rate of 0.8908850. Furthermore, alternative optimisation algorithms may be incorporated to enhance efficiency in physical layer security.

References

[1]. Pooja Singh and Aditya Trivedi, "NOMA and massive MIMO assisted Physical Layer Security using Artificial Noise precoding", Physical Communication, vol.39, pp.100977, 2020.

[2]. P. Chandra Sekhar, T. S. N. Murthy, "Physical Layer Security using SMO" 2022 IEEE-International Conference on Computing, Communication and Power Technology (IC3P)-2022.

[3]. T.S.N. Murthy, P. Chandra Sekhar, Srinivasa Sastry G, "Physical Layer Security using Squirrel Search Algorithm", IEEE International Symposium on Circuits and Systems (ISCAS)-2023.

[4]. P. Chandra Sekhar, T. S. N. Murthy, "RSMO: Rider Spider Monkey Optimization-based artificial noise precoding technique for Physical Layer Security in 5G networks", Wireless Personal Communications journal, Vol.135, pp 2355–2377, (2024), https://doi.org/10.1007/s11277-024-11166-4.

[5]. Huiqing Bai, Liang Jin, and Ming Yi, "Artificial Noise Aided Polar Codes for Physical Layer Security", China Communications, vol.14, no.12, pp.15-24, 2017.

[6]. Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", In proceedings ofthe IEEE, vol. 104, no. 9, pp. 1727-1765, 2016.

[7]. X. M Chen, W. K Ng, W. Gerstacker, et al, "A Survey on Multiple-antenna Techniques for Physical Layer Security," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, 2017, pp.1027-1053.

[8]. A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, October 1975.

[9]. P. Singh, P. Pawar, and A. Trivedi, "Physical layer security approaches in 5G wireless communication networks," In proceedings of First International Conference on Secure Cyber Computing and Communication (ICSCCC), NIT Jalandhar, pp. 477–482, December 2018.

[10]. S. Ata, "Secrecy performance analysis over cascaded fading channels," IET Communications, vol. 13, no. 2, pp. 259–264,2019.

[11]. Hui-Ming Wang, Tong-Xing Zheng, Jinhong Yuan, Don Towsley, and Moon Ho Lee, "Physical Layer Security in Heterogeneous Cellular Networks", IEEE Transactions on Communications, vol.64, no.3, pp.1204-1219, 2016.

[12]. Huiqing Bai, Liang Jin, and Ming Yi, "Artificial Noise Aided Polar Codes for Physical Layer Security", China Communications, vol.14, no.12, pp.15-24, 2017.

[13]. Hayder Al-Hraishawi, Gayan Amarasuriya Aruma Baduge, and Rafael F. Schaefer, "Artificial Noise-Aided Physical Layer Security in Underlay Cognitive Massive MIMO Systems with Pilot Contamination", Entropy, vol.19, vol.7, p.349, 2017.

[14]. Raj Kumar Patra, P. Chandra Sekhar, etc "User-segregation based channel estimation in the MIMO system" Physical Communication-Elsevier, Volume 56, February 2023,-https://doi.org/10.1016/j.phycom.2022.101971.

[15]. L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," IEEE Wireless Communications and Mobile Computing Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2294– 2323, 2018.

[16]. Y. Chen, A. Bayesteh, Y. Wu et al., "Toward the standardization of non-orthogonal multiple access for next generation wireless networks," IEEE Communications Magazine, vol. 56, no. 3, pp. 19–27, 2018.

[17]. Zhijin Qin, Yuanwei Liu, Zhiguo Ding, Yue Gao, and Maged Elkashlan," Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks", In 2016 IEEE International Conference on Communications (ICC), IEEE.pp. 1-6, 2016.

[18]. N. Fatema, G. Hua, Y. Xiang, D. Peng, and I. Natgunanathan, "Massive MIMO linear precoding: A survey," IEEE Systems Journal, vol. 12, no. 4, pp. 3920–3931, Dec 2018.

[19]. F. Hasegawa, H. Nishimoto, N. Song, M. Enescu, A. Taira, A. Okazaki, and A. Okamura, "Non-linear precoding for 5G NR," In proceedings of IEEE Conference on Standards for Communications and Networking (CSCN), Paris (France), pp.1-7, October2018.

[20]. I. Csisz´ar and J. K¨orner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[21]. X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secret communication," in *Proc. IEEE Inform. Theory Workshop (ITW)*, Porto, Portugal, May 2008, pp. 164–168.

[22]. R. Negi and S. Goel, "Secret communications using artificial noise," in *Proc. IEEE Veh. Tech. Conf. (VTC)*, Dallas, TX, Sept. 2005, pp. 1906–1910.

[23]. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[24]. A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. on Acoustic, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[25]. Muhammad R. A. Khandaker, Christos Masouros and Kai-Kit Wong, "Constructive Interference Based Secure Precoding: A New Dimension in Physical Layer Security", IEEE Transactions on Information Forensics and Security, vol.13, no.9, pp.2256-2268, 2018.

[26]. Hayder Al-Hraishawi, Gayan Amarasuriya Aruma Baduge, and Rafael F. Schaefer, "Artificial Noise-Aided Physical Layer Security inUnderlay Cognitive Massive MIMO Systems with Pilot Contamination", Entropy, vol.19, vol.7, p.349, 2017.

[27]. Zhijin Qin, Yuanwei Liu, Zhiguo Ding, Yue Gao, and Maged Elkashlan," Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks", In 2016 IEEE International Conference on Communications (ICC), IEEE.pp. 1-6, 2016.

[28]. Jun Zhu, Robert Schober, and Vijay K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems", IEEE Transactions on Wireless Communications, vol.15, no.3, pp.2245-2261, 2015

[29]. Yanjun Chen, Xinsheng Ji1, Kaizhi Huang, Jing Yang, Xin Hu, and Yunjia Xu, "Artificial noise-assisted physical layer security in D2D-enabled cellular networks", EURASIP Journal on Wireless Communications and Networking, vol.1, pp.1-15, 2017.

[30]. M. H. Kabir, S. Z. Rashid, A. Gafur, M. N. Islam, and M. J. Hoque, "Maximum energy efficiency of three precoding methods for massive MIMO technique in wireless communication system," In proceedings of International Conference on Electrical, Computer and Communication Engineering (ECCE), Bangladesh, pp. 1–5, February 2019.

[31]. Jun Zhu, Robert Schober, and Vijay K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems", IEEE Transactions on Wireless Communications, vol.15, no.3, pp.2245-2261, 2015.

[32]. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180–2189, June 2008.

[33]. Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system," IEEE Access, vol. 7, pp. 58 353–58 360, 2019.