International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10714-10721

Fast Iterative Channel Estimation with Original Symbol Phase Rotated Secure Transmission against Powerful Massive MIMO Eavesdropper

Gurpreet Kaur Kohli*, Prof. Kiranpreet Kaur**

**M.tech Scholar, Department of Electronics and Communication Engineering, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India.*

***Assistant Professor, Department of Electronics and Communication, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India.*

Abstract

The major concern involved in multiple-input multiple-output (MIMO) is considered to be the presence of eavesdroppers equipped with large antenna arrays. These eavesdroppers may attempt to intercept the confidential information of users during transmissions. The objective of the proposed work is to obtain significant amount of security at physical layer transmissions. The existing approaches addressed the security issue by applying various beam forming techniques for processing the original signal. These conventional approaches failed to resolve issue as they provided low secrecy rate. Therefore, the proposed work suggested the use of Original Symbol Phase Rotated (OSPR) with Fast Iterative Channel Estimation Algorithm. Under this technique the original phase of the signal was rotated randomly before it was transmitted. This disabled the eavesdroppers to intercept the original signal phase while the authorized users were able to infer the correct phase of signal for performing inverse operations for decoding the received signal. The iterative compensation algorithm is used due its feature that detects the noise and also deals with the distorted signals in an iterative manner. Hence the information in the signal remains noiseless and meaningful. The result obtained verifies high efficiency of proposed technique in terms of Signal to Noise Ratio (SNR) and Symbol Error Rate (SER). The comparison between traditional OSPR and proposed OSPR with fast iterative channel estimation algorithm is also analyzed in this work. On the basis of the comparison study the proposed work is observed to be more efficient than traditional OSPR technique in respective parameters.

Keywords: OSPR, SNR, SER, BS and Fast correlated channel estimation with iterative compensation.

INTRODUCTION

The analysis of MIMO systems shows that increasing number of antennas leads to higher performance gains. In case of large dimensions of the system generation of certain processing overheads may occur. The reason behind such overhead generation is considered to be properties of large dimension matrices involved in large dimension MIMO systems. The figure below shows the simplified model of massive MIMO system based on matched filter which is required for the accomplishing detection process. Figure 1 shows a single base station which serves two single antenna users simultaneously. Each channel user is represented by $h_i \in \mathbb{C}^{N_a \times 1}$.

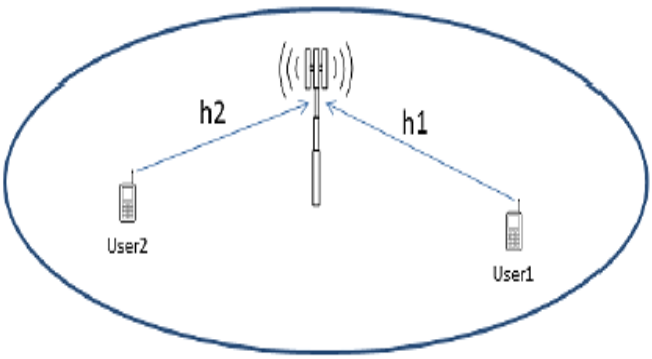


Figure 1. A simple model for single base station [6]

Here, the total numbers of antennas present at base station are given by N_a. Each entry of h_i is distributed by Gaussian distribution having zero valued mean and unit variance [6]. An assumption is made during this by which it is considered that knowledge regarding the state of channels is known at base station. The received signal is evaluated by using the following equation (1):

$$y = h_1 x_1 + h_2 x_2 + w \ldots . (1)$$

Where, n represents the noise vector and $n \sim CN(0,1)$. By the application of simple matched filter by BS the transmitted symbol of user1 is detected [7]. The matched filter for user 1 is obtained by the expression z: $\frac{1}{h_1} {h_1}^n$. This is followed by the Evaluation of the product of detection vector and $\frac{|h_i|}{N_n}$. The performance is given by the below equation (2)

Desired | Interference | Noise

$$\frac{1}{N_a} h_1^H y = x_1 \frac{1}{N_a} \sum_{k=1}^{N_a} \left(|h_{1,k}|^2 \right) + x_1 \frac{1}{N_a} \sum_{k=1}^{N_a} \left(h_{1,k}^* h_{2,k} \right) + x_1 \frac{1}{N_a} \sum_{k=1}^{N_a} \left(h_{1,k}^* w_k \right) \dots\dots (2)$$

The performance is not affected by detection vector. The process of detection for detecting the user 1's symbol is hindered by the interference and noise parts of the equation. As per the law of large number if N_a approaches to infinity i.e. $N_a \to \infty$ the values of interference is given as $E\left[h_{1,k}^* h_{2,k}\right]$ and noise part is obtained by $E\left[h_{1,k}^* w_k\right]$.

Due to the uncorrelated elements present in the expectations it is considered to be of zero valued due to which they are neglected in detected signal.

$$\frac{1}{N_a} h_1^H y = x_1 \frac{1}{N_a} \sum_{k=1}^{N_a} (|h_{1,k}|^2) \to x_1 E\left[|h_{1,k}|^2\right] = x_1 \dots\dots (3)$$

The increased system dimensions leading to processing simplifications are shown in the given equation above. For checking the user data in uplink a simple matched filter can be employed as no undesired and uncorrelated parts are involved in it which simplifies the task. Massive MIMO systems are formed by connecting huge number of base station antennas with numerous users due to which it is considered as a form of MU-MIMO systems[6][7].

At the same frequency resource thousands of users can be served simultaneously by hundreds or thousands of antenna arrays at base station employed in massive MIMO.

PROBLEM FORMULATION

After having a review to the traditional work in the domain of security in Massive MIMO communication system, it is observed that various authors have developed different methods to secure the communication system from malicious attacks like eavesdropping etc. The major problem that have been seen in the traditional work is that the imperfection of CSI often focuses on the receiver side sometimes leads to an error in the amplitude and phase of the signals during the process of demodulation and decoding. This indirectly affects the errors and imperfection in channel estimation. Thus, there is a need to improve this mechanism by developing an enhanced method for it.

PROPOSED WORK

The above section gives an overview to the backlog of the traditional work which motivates to develop a new mechanism for securing and enhancing the performance of massive MIMO communication system. In proposed work a v channel estimation algorithm is designed to achieve the urate channel estimation. Along with this, a fast relation algorithm is also implemented on the basis of the ative compensation; the iterative compensation algorithm used with a motive to overcome the errors of fast relation algorithm and when iterative compensation nbined with fast correlation algorithm improves the klogs of traditional system. The steps involved in the posed methodology are given below:

) 1: First step is to generate a signal. The signal generation one randomly and this generated signal is used for further cessing.

Step 2: In this step, the generated signal is modulated over sub-carriers which consume very small portion of bandwidth. The signal modulation is done by using modulation techniques. After modulation, the effect of noise is applied to the modulated signal.

Step 3: Apply fast correlated channel estimated algorithm for channel estimation.

Step 4: In this the iterative compensation is applied to the signal that is generated after applying fast correlated channel estimation algorithm to reduce and calculate the errors produced by fast channel correlated estimation algorithm. Through iterative compensation the losses produced during the signal propagation are reduced.

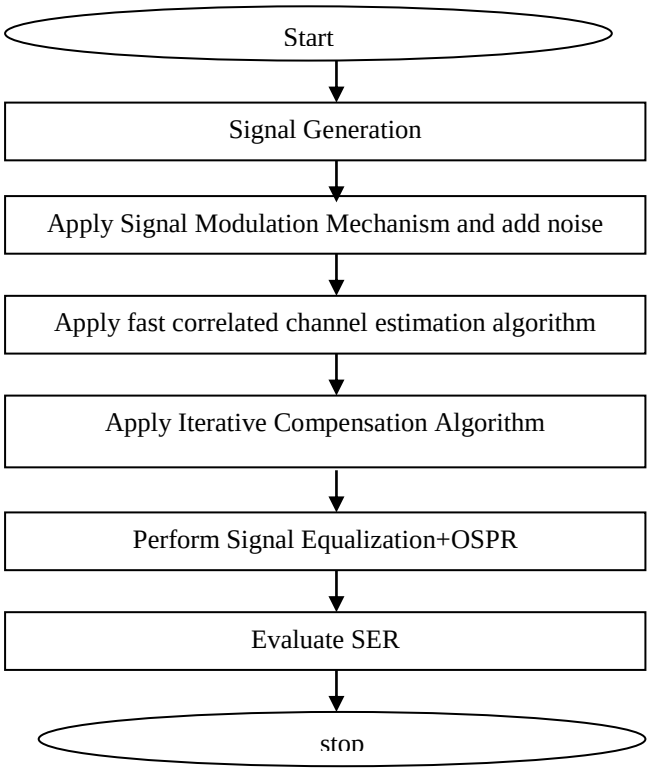


Figure 2. Block Diagram of proposed work

Step 5: The signal equalization is performed after applying the compensation mechanism as it is essential to reduce amplitude and delay distortions which may lead to Inter-Symbol Interference (ISI). In this step the OSPR (Original Symbol

Phase Rotated) is applied so that the secure data transmission can be done

Step 6: At last the system performance is evaluated by measuring the Symbol Error Rate (SER) of the output signals.

System Model

Fast Correlated Channel Estimation Algorithm

The mathematical model for Fast Correlated Estimation algorithm is defined in this section. The figure 3 below represents the working of fast correlated channel estimation algorithm [16].

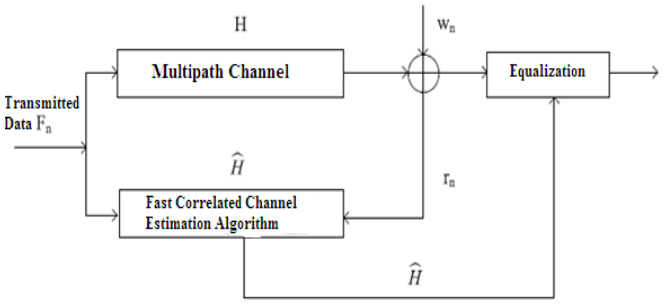


Figure 3. Theory of Fast Correlated Channel Estimated Algorithm [16]

In fast correlated channel estimation, after applying Binary Phase Shift Key (BPSK) modulation, the training sequence defined in equation (4) below [16] is transmitted by using a multipath channel with the addition of additive noise ω_n to it.

$$F_n = [f_n, f_{n+1}, \dots \dots . f_{n+l}] \dots \dots \dots (4)$$

Where, l denotes the length for the memory of a multipath channel. The structure of received signal r_n is represented in equation (5).

$$r_n = F_n H^T + \omega_n = \sum_{k=0}^{L} f_{n-k} h_k + \omega_n \dots \dots . . (5)$$

h_k Denotes the k_{th} path for multipath channel parameter H. L is used to define the number of sub paths of multipath channel. ω_n Represents the white Gaussian noise along with 0 mean and σ^2 variance [16]. The correlation function can be calculated as follows:

$$\mathbb{E}[r_n f_{n-k}] = \mathbb{E}[h_k f_{n-k} f_{n-k}] + \sum_{\substack{j=0 \\ j \neq k}}^{L} \mathbb{E}[h_j f_{n-k} f_{n-j}] + \mathbb{E}[\omega_n f_{n-k}] \quad \dots . (6)$$

$$h_k = \frac{\mathbb{E}[r_n f_{n-k}]}{\mathbb{E}[f_{n-k} f_{n-k}]} \quad \dots . (7)$$

From equation (7), it is observed that the f_{n-k} and ω_n are uncorrelated which proves that the algorithm is highly efficient to prevent the signals form noise.

Fast Correlated Channel Estimation algorithm based on iterative compensation

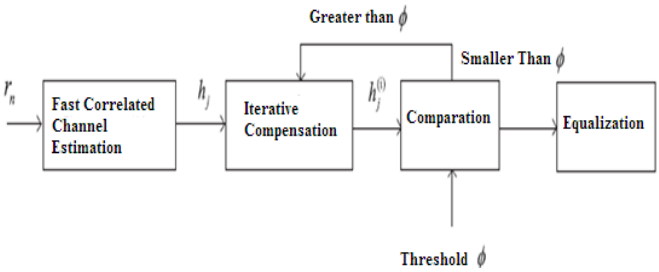


Figure 4. Working of Iterative Compensation Algorithm [16]

Equation (8) is derived [16] to evaluate the accurate estimate h_k which should be equivalent to the multipath channel parameters:

$$\hat{h_k} = h_k - \frac{1}{N} \sum_{\substack{j=0 \\ j \neq k}}^{L} h_j + \frac{1}{N} E[w_n f_n - k] \dots . (8)$$

The estimated error of fast correlated channel is described in following formulation

$$\zeta = \frac{1}{N} \sum_{\substack{j=0 \\ j \neq k}}^{L} h_j \dots . (9)$$

Another parameter i.e. noise error of fast correlated channel estimation is defined as follows:

$$\psi = {}^{\mathrm{E}[w_n f_n - k]}/_{N} \dots . . (10)$$

The following equation expresses the equation (18).

$$\hat{h_k} = h_k - \zeta - \psi \dots (11)$$

Here in equation 8, 9, 10 and 11, ζ denotes the estimation error, ψ denotes the noise error generated by the channel [16].

RESULTS

In this section, evaluation of the security performance for the fast correlated channel estimation secure transmission scheme and simulation results are represented.

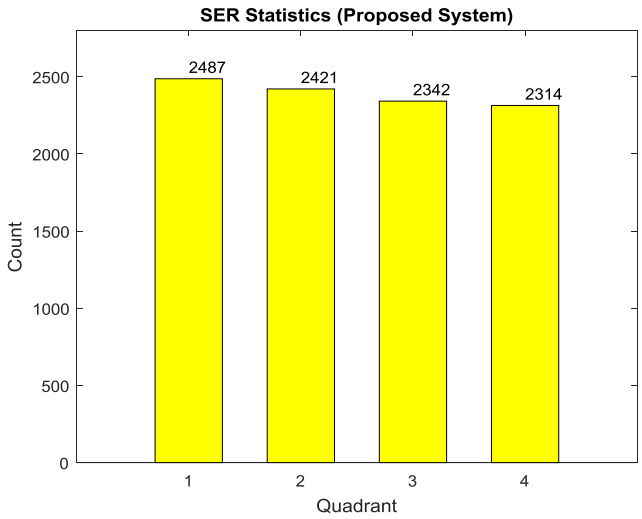


Figure 5. Symbol Error Rate (SER) statistics of Massive MIMO

The antennas used for the evaluation are varying from 64 to 1024. Symbol used for their representation is N_b. Their numbers are large enough for the proper working. The x axis in figure 5 denotes the quadrant where the intercepted symbols fall in. The y axis calibrates the data for count that ranges from 0 to 3000. On the basis of the obtained graph, it is observed that for first quadrant, 2487 symbols are intercepted by the Massive MIMO eavesdropper whereas, for other quadrants the relative value is small. The high SER value depicts the decrement of the recovered information and also confirms the security performance for proposed scheme.

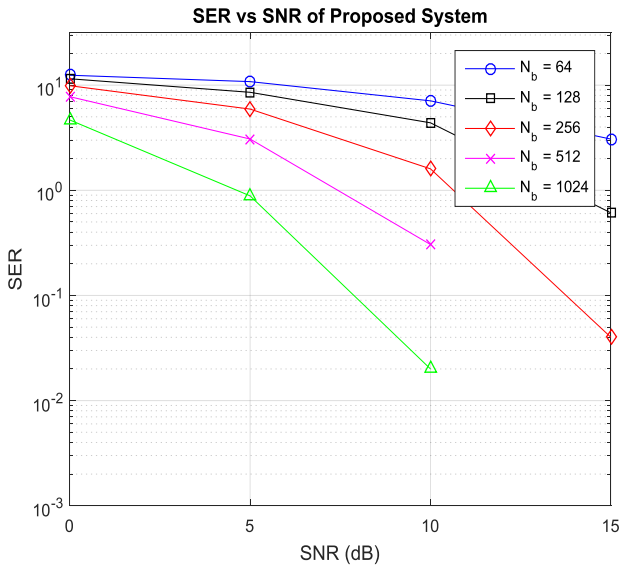


Figure 6. SER of Kth User Terminal

In the figure 6, SER of Kth user terminal is plotted where different BS antennas such as 64, 128, 256, 512 and 1024 are considered. From the result acquired, it can be seen that as the number of BS antennas increases, the performance of SER becomes better. Thus, performance of the system is enhanced with proposed scheme as compared to OSPR. Moreover, increasing SNR cannot effectively improve the performance of SER, when the number of BS antennas is not large enough compared with the number of served User Terminals. Additionally, in figure, SER of massive MIMO eavesdropper is high while the massive MIMO BS can work properly and original symbols can be recovered through UTs.

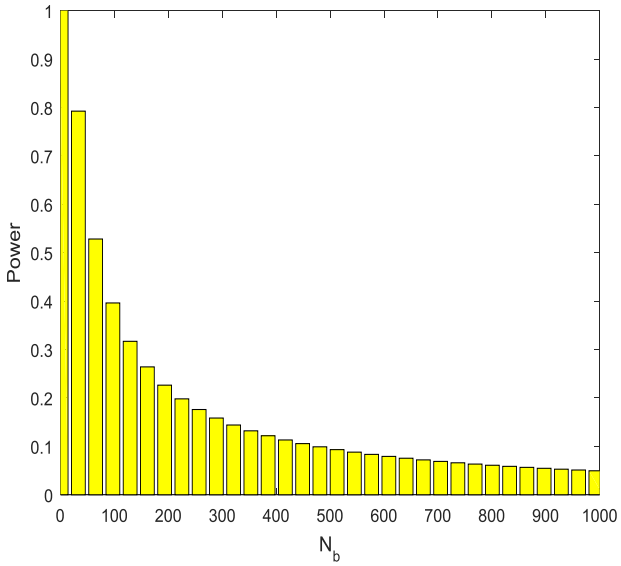


Figure 7. Total radiated power of the Massive MIMO BS

The figure 7 shows that total radiated power of the massive MIMO BS as a function of the number of BS antennas N_b. The x axis in the graph represents the number of base stations and y axis shows the amount of power consumed. From the result acquired, it is shown that consumption of power decreases with the increased number of BS antennas N_b. The plotted result confirmed that more BS antennas provided better energy efficiency in wireless system.

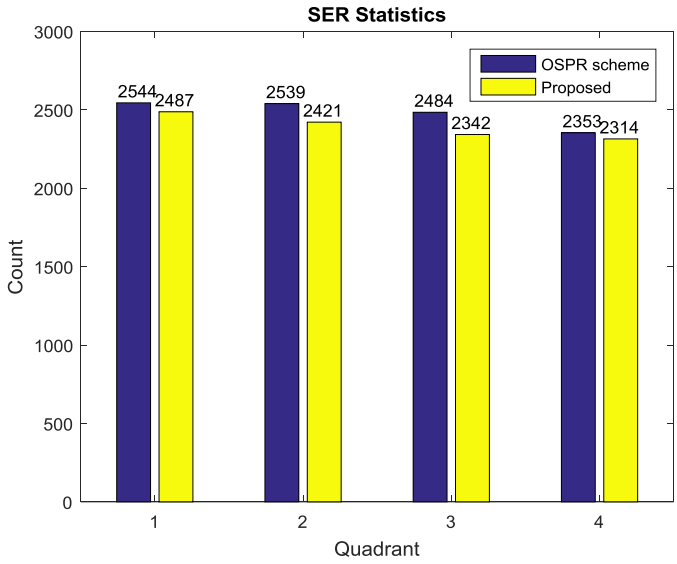
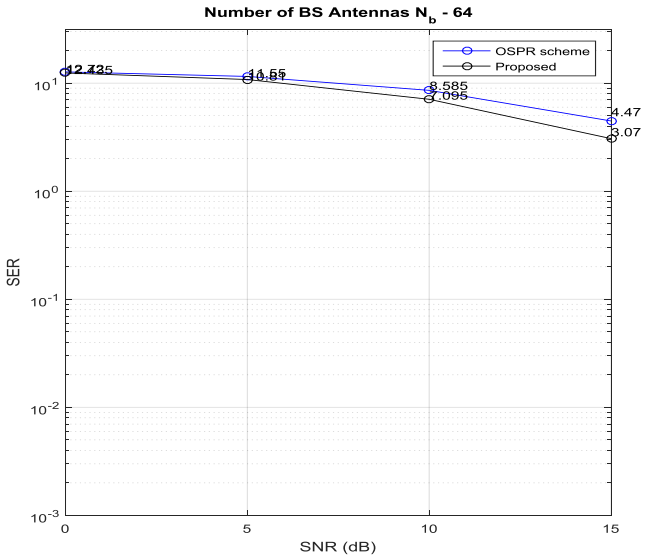


Figure 8. Comparison of Proposed and OSPR Scheme

The figure 8 depicts the comparison of proposed and traditional OSPR scheme on the basis of Interception symbols. The x axis calibrates the data in the form of quadrants where the intercepted symbol falls. The y axis depicts the counts. The graph proves that the 2544 symbols are intercepted by the massive MIMO in OSPR scheme corresponding to first quadrant whereas the relative value is 2487 for proposed work which depicts proposed scheme is better than OSPR because lesser the intercepted symbols higher the SER of eavesdropper indicates great reduction of successfully recovered original information .

Table 1. SER statistics with respect to Quadrants

Technique	Parameters	Quadrant 1	Quadrant 2	Quadrant 3	Quadrant 4
Proposed Scheme	Intercepted symbols	2487	2421	2342	2314
OSPR Scheme	Intercepted symbols	2544	2539	2484	2353

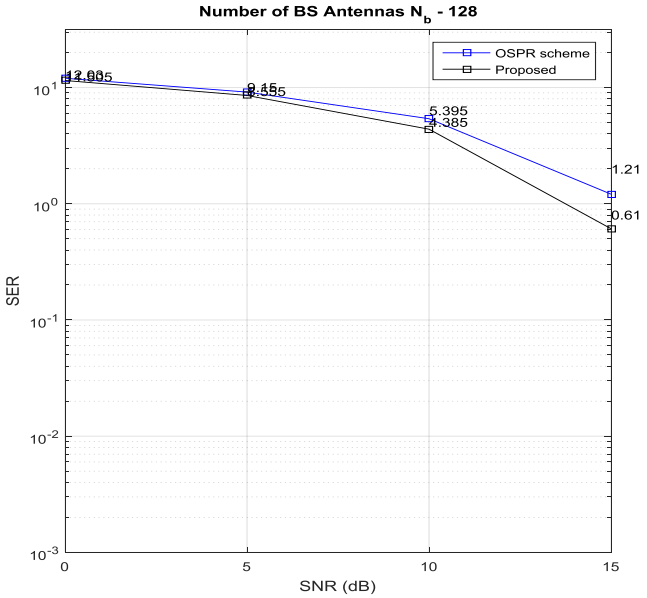


(a) 64 Base station Antennas

Figure 9. SER of System with (a) 64 Base station Antennas

Table 2. SER for Massive MIMO with 64 base station antennas

Technique	Parameters	Values			
Proposed	SNR	0	5	10	15
	SER	12.44	10.81	7.095	3.07
OSPR Scheme	SNR	0	5	10	15
	SER	12.72	11.55	8.585	4.47

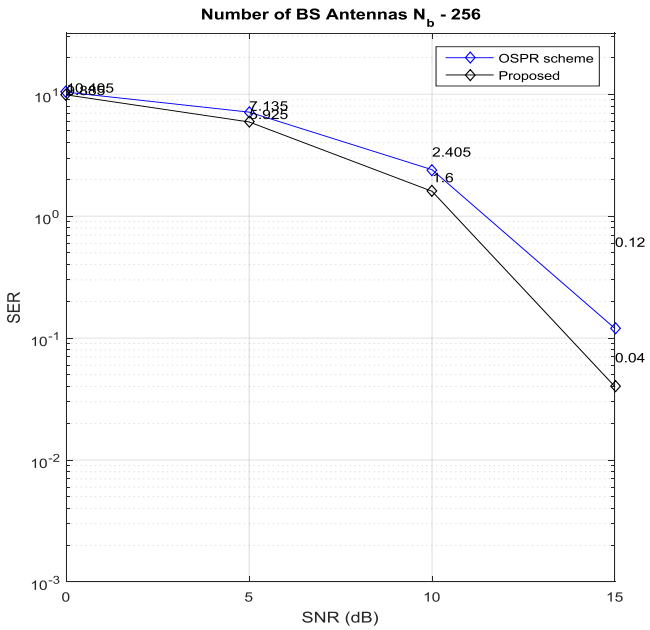


b) 128 Base station Antennas

Figure 10. SER of System with (b) 128 Base station Antennas

Table 3. SER for Massive MIMO with 128 base station antennas

Technique	Parameters	Values			
Proposed	SNR	0	5	10	15
	SER	11.51	8.555	4.385	0.61
OSPR Scheme	SNR	0	5	10	15
	SER	12.03	9.15	5.395	1.21

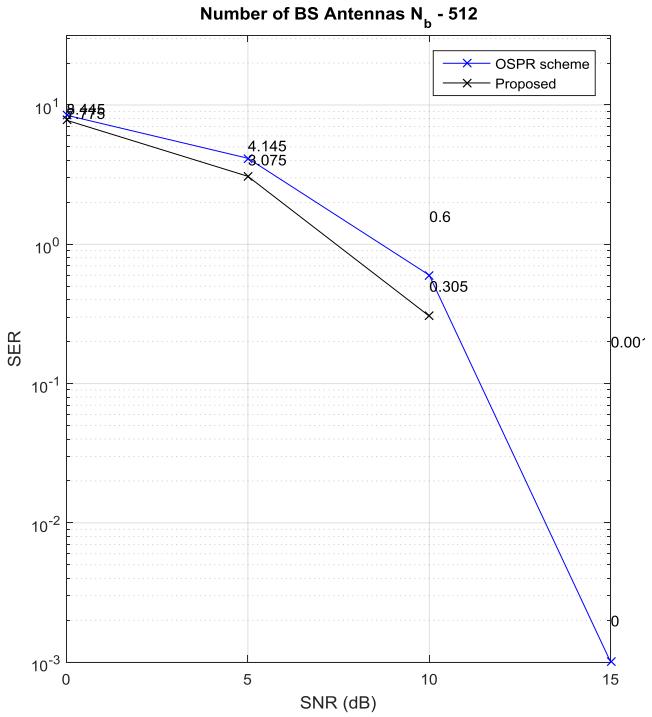


(c) 256 Base station Antennas

Figure 11. SER of System with (c) 256 Base station Antennas

Table 4. SER for Massive MIMO with 256 base station antennas

Technique	Parameters	Values			
Proposed	SNR	0	5	10	15
	SER	9.885	5.925	1.6	0.04
OSPR Scheme	SNR	0	5	10	15
	SER	10.4	7.135	2.405	0.12

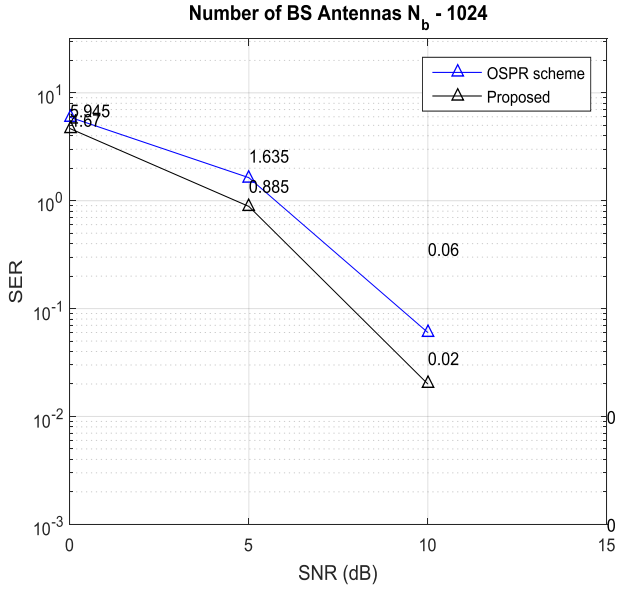


d) 512 Base station Antennas

Figure 12. SER of System with (d) 512 Base station Antennas

Table 5. SER for Massive MIMO with 512 base station antennas

Technique	Parameters	Values			
Proposed	SNR	0	5	10	15
	SER	7.775	3.075	0.305	0
OSPR Scheme	SNR	0	5	10	15
	SER	8.445	4.145	0.6	0.001



(e) 1024 Base station Antennas

Figure 13. SER of System with (e) 1024 Base station Antennas

Table 6. SER for Massive MIMO with 1024 base station antennas

Technique	Parameters	Values			
Proposed	SNR	0	5	10	15
	SER	4.67	0.885	0.02	0
OSPR Scheme	SNR	0	5	10	15
	SER	5.945	1.635	0.06	0

Table 2, 3, 4, 5 and 6 depict the comparison of SER of proposed and traditional OSPR scheme. The table 2, 3 and 4 comprised of the facts that represent the SER of Massive MIMO with respect to 64, 128 and 256 base antennas and table 5 and table 6 shows the SER of proposed and OSPR scheme for 512 and 1024 base antennas respectively. On the basis of facts that are shown in tables below, it is proved that the SER of proposed scheme is better than the OSPR scheme. The SER is evaluated on the basis of SNR. The corresponding graphical results shown in figure 9, 10, 11, 12 and 13 respectively also depict proposed scheme is better than the OSPR scheme.

CONCLUSION

Multiple-Input Multiple-Output (MIMO) technology is a topic of concern from the past twenty years because it is proved to be efficient in terms of reliability and capacity of the wireless systems. In massive MIMO, multi-user MIMO (MU-MIMO) systems are where base stations are equipped with a large number (say, tens to hundreds) of antennas. With this terminology, experiments have performed to evaluate the energy efficiency of the system.

In the Traditional work, a novel secure transmission scheme called OSPR (Original Symbol Phase Rotated) was proposed to defend against eavesdroppers armed with massive antennas in a single-cell scenario. The OSPR secure transmission scheme was introduced step by step. The corresponding security performance was comprehensively investigated under certain assumptions. Practical simulation results with finite alphabet QPSK inputs were provided to further corroborate the effectiveness of the OSPR scheme. It was shown that as long as the BS is equipped with a sufficient number of antennas, the powerful massive MIMO eavesdropper will not be able to recover most of the original symbols (i.e., the SER is high), even if it has an infinite number of antennas, while the legitimate UTs were able to correctly recover the original symbols. Thus the security performance of the system was guaranteed to a large extent. Moreover, it was shown that the OSPR scheme does not affect the high energy efficiency of the massive MIMO BS, and it involves no jamming like approach which is power consuming. This makes the OSPR scheme a good candidate for green and secure transmissions.

In Present work as Massive multiple-input multiple-output technology is considered to be highly efficient in providing effective wireless communication. The large number of antenna arrays employed in it is capable of providing its service to multiple users at same instant of time. The presences of eavesdroppers that attempt to intercept the information in the uplink are restricted even after phase rotation by OSPR scheme because due lack of perfection in channel estimations there was a problem in detection and decoding process as these imperfections in estimation may lead to errors in rotated phase so by employing the proposed technique this problem can be resolved. In this work, the work of OSPR is used to retain the privacy of data. Along with this, the fast correlated channel estimation algorithm was proposed based on iterative compensation. This algorithm is used for reduction of errors, distortion, channel capacity enhancement, to get perfect CSI, perfect channel estimation along with multi-cell scenario. On the basis of the results that are obtained after simulation, it is concluded that result in SER statistics of massive MIMO depicted counts verses quadrant graph where within each quadrant the count of symbols intercepted by eavesdropper in each quadrant decreases which increase the SER of eavesdropper and hence depicts the decrement of the recovered information thus increasing security performance of for proposed scheme. The SER of Kth terminal depicts the graph of Symbol Error Rate (SER) verses Signal to Noise Ratio (SNR) of proposed work is efficient in comparison to the traditional work because at every power level the value of SER is decreasing.

In the graph of total radiated power of the massive MIMO BS, the power is decreasing with increase in no of BS antennas. In all comparison graphs the values of proposed algorithm are better and improved than the traditional OSPR scheme. Hence proposed work outperforms the traditional work.

In future, the present results can be enhanced more by applying Artificial Intelligence (AI) based optimization techniques. The optimized results lead a system to take more reliable and efficient decisions. Thus, the introduction of optimization technique can enhanced the quality of results as well.

REFERENCES

[1] G. Aamarasurya and R.F. Shaefer, "Secure Transmission in Cognitive Massive MIMO Systems with Underlay Spectrum Sharing", 9th International Symposium on Turbo Codes & Iterative Information Processing, pp. 380-384, 2016.

[2] G. Anjos, D. Castanheira, A. Silva, A. Gameiro, M. Gomes and J. Vilela, "Joint Design of Massive MIMO Precoder and Security Scheme for Multiuser Scenarios under Reciprocal Channel Conditions", Wireless Communications and Mobile Computing, pp. 1-10, 2017.

[3] H. Al-Hraishawi, G. Amarasuriya and R.F. Schaefer, "Secure Communication in Underlay Cognitive Massive MIMO Systems with Pilot Contamination", (GLOBECOM) IEEE Global Communications Conference, pp. 1-7, 2017.

[4] B. Chen, C. Zhu, W. Li, J. Wei, V.C. M. Leung and L.T. Yang, "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper", Vol. 4, pp. 3016-3025, 2016.

[5] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V.C. M. Leung and J.J. P. C. Rodrigues, "Securing Uplink Transmission for Lightweight Single-antenna UEs in the Presence of a Massive MIMO Eavesdropper", IEEE, Vol. 4, pp. 2169 – 3536, 2016.

[6] X. Chen, J. Chen and T. Liu, "Secure Transmission in Wireless Powered Massive MIMO Relaying Systems: Performance Analysis and Optimization", Vol. 65, pp. 8025 – 8035, 2016.

[7] T. Dean and A. Goldsmith, "Physical-Layer Cryptography through Massive MIMO", Information Theory Workshop (ITW), IEEE, pp. 1-5, 2013.

[8] Y. Deng, L. Wang, K. Wong, A. Nallanathan, M. kashlan and S. Lambotharan, "Safeguarding Massive MIMO Aided HetNets Using Physical Layer Security", Wireless Communications & Signal Processing (WCSP), International Conference, pp. 1-5, 2015.

[9] K. Guo, Y. Guo and G. Ascheid, "Distributed Antennas Aided Secure Communication in MU-Massive-MIMO with QoS Guarantee", Vehicular Technology Conference (VTC Fall), IEEE 82nd, pp. 1-7, 2015.

[10] K. Guo, Y. Guo and G. Ascheid, "Security-Constrained Power Allocation in MU-Massive-MIMO with Distributed Antennas", IEEE, Vol. 15, pp. 8139 – 8153, 2016.

[11] J. Gangane and P. Somaiyal, "A Review on Massive MIMO for Next Generation Wireless Communication Systems", International Journal of Current Engineering

and Scientific Research (IJCESR), Vol. 3, Issue 7, pp. 56-60, 2016.

[12] T. Hoang, T. Duong, H. Tuan and H. Vincent Poor, "Secure Massive MIMO Relaying Systems in a Poisson Field of Eavesdroppers", IEEE Transactions on Communications, Vol. 65, pp. 4857 – 4870, 2017.

[13] V. Korzhik, G. Morales-Luna, S. Tikhonov and V. Yakovlev, "Analysis of Keyless Massive MIMO-based Cryptosystem Security", IACR, 2015.

[14] B. Li, L. Lei Li, D. He, J. Chen and W. Kong, "Energy-Efficient Secure Transmission in Massive MIMO Systems with Pilot Attack", Wireless Communications & Signal Processing (WCSP), 8th International Conference, pp. 1-5, 2016.

[15] X. Li, Y. Zhang and W. Cadeau, "Hybrid Massive MIMO for Secure Transmissions against Stealthy Eavesdroppers", Vol. 22, pp. 81 – 84, 2018.

[16] Z. Li, Y. Li, D. Wang and L. Yao, "A Novel Channel Estimation Algorithm Based on Iterative Compensation", IEEE Transactions and Broadcasting, pp.1-8, 2016.

[17] W. Ni, X. Dong and W. Sheng Lu, "Near-Optimal Hybrid Processing for Massive MIMO Systems via Matrix Decomposition", IEEE transactions on signal processing, Vol. 65, pp. 3922-3933, 2017.

[18] N. Romero-Zurita, M. Ghogho and D. McLernon, "Physical layer security of MIMO–OFDM systems by beam forming and artificial noise generation", Elsevier Physical Communication, Vol. 4, pp. 313–321, 2011.