ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

The Secrecy Capacity Region of MIMO Multi-Receiver Wiretap Channel

Neeraja N[1]

PG Student, Dept. of AE&CS, Cochin College of Engineering and Technology, Valanchery, Kerala, India[1]

ABSTRACT: The main advantage of MIMO system is that it can transmit and receive different signals over multiple antennas and OFDM can provide efficiency to deal with multipath .Here in this project we are going to combine an MIMO system with OFDM to provide a more reliable network with greater speed and range. At the same time we are also providing data secrecy at the physical layer. For this we are taking two cases: when full channel state information of the receiver is know and the second case is that we know only partial information about the CSI of the receiver. Further we are going to implement the system and compare the performance ie, the secrecy, reliability, speed and range of this proposed system with the existing system which uses only the MIMO. Based on the analysis we can conclude that this system achieves desired results.

KEYWORDS: MIMO,OFDM, CSI

I. INTRODUCTION

The future world is going to depend highly on the wireless communication. So we are in need of developing a system which can provide high speed, reliability, and range. This system should be also able to provide high security also.

Now we are going to analyse existing system [1], here they are evaluating two cases ie, when the CSI information of the legitimate receiver is known to the transmitter and when partial CSI is known to the legitimate receiver. In the first case they are proposing a pre-coder to increase the SNR value and to attain the secrecy, in the second case they are going to modify the Lloyds algorithm and propose a pre-coder and post-coder.

Here in this project we are going to combine a MIMO-OFDM system in-order satisfy the needs of future generation. In this system we are going to increase the capacity of the secrecy region. This is done by taking two OFDM signals in high traffic condition and transmitting through a MIMO system. Here we are going to take the calculations at the peak time in-order to show the efficiency.

From the computations it is shown that this system provides secrecy and at the same time increases the transmission rate, range and BER value.

II. PROPOSED SYSTEM

Now we are going to implement a system which provides good secrecy and at the same time increases the transmission rate, range and BER value.

For this we are combining MIMO with OFDM in a high traffic environment. For this first are taking 4 transmitters and the receiver system.

In the transmission side first of all we are going to implement a precoder. In this precoder we are going to implement the modified Lloyds algorithm. In the receiver side a low complexity postcoder is implemented to maintain the SNR

DOI:10.15662/IJAREEIE.2019.0803098

value. Thus we are going to optimally utilise the secrecy region which in turn increases the capacity of the secrecy region.

III. IMPLEMENTATION OF THE SYSTEM

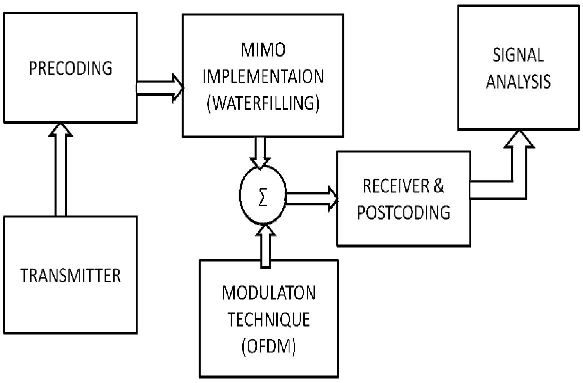

Fig 3.1 block diagram of proposed system

The above given diagram shows the basic block diagram of the system. Here it consists of a transmitter which is used for transmission of data. Then we have a precoder section where we are going to implement the codings, here we are using modified Lloyds algorithm inoder to maintain secrecy. The optimal code word Cα which is to be used for the development of the codings is given by

Cα=eigenvectors corresponding to the R largest centroid values

So from the data of the four transmitters we will obtain the optimal code word which is nearer to the centroid values. Also the Lloyds algorithm is used for the compression of the data which inturn increases the transmission rate.

After obtaining the precoding now we are implementing the system using water filling algorithm in MIMO system. From the algorithm we are taking the final signal as

P_{total}=sum of all vectors above water level.

Here since we are going to implement many signals along with noise we are taking

P_{total1}=avg of P_{total}

Thus with the help of the above given we will obtain a normalised signal.

IV. ANALYSIS AND SIMULATION RESULTS

In this section we are going to analyse the performance of the MIMO system with MIMO-OFDM system.
First we are going to take a OFDM signal and calculate its peak during transmission at a high traffic condition.

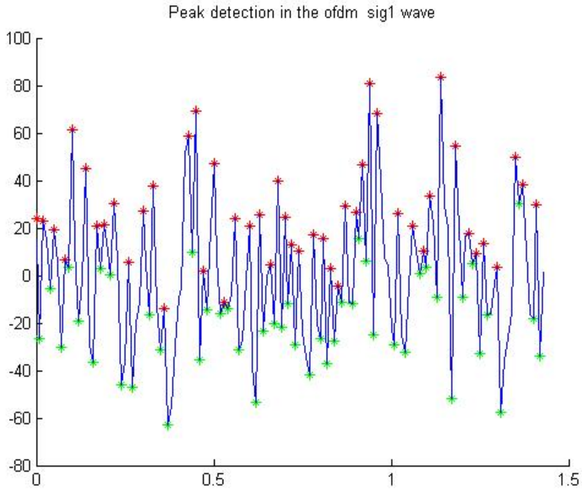

Fig.4.1 Peak detection of the signal through MIMO-OFDM

Now we are going to analyse the secrecy region occupied for the normal MIMO system and the modified MIMO-OFDM system.

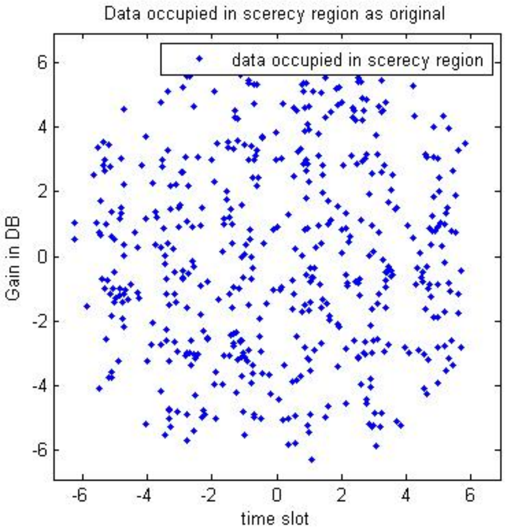

Fig.4.2 general occupation of data in secrecy region-MIMO system.

This above given figure shows how data is occupied in a normal system. From this it is easily understood that the scattered occupation consumes the major area.

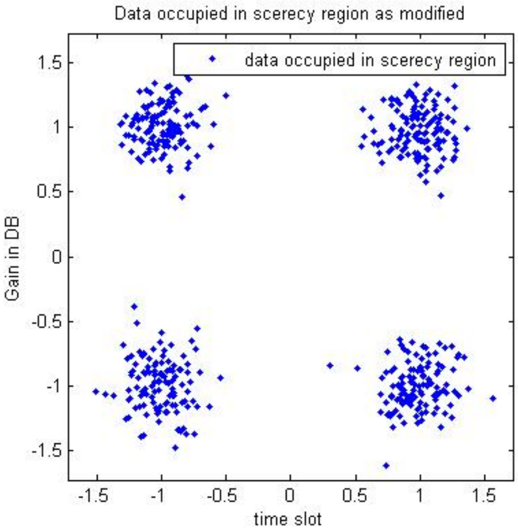

Fig.4.3 data occupied in secrecy region of modified system.

From the above given figure it is found that data is compressed in such a way that in a single time slot more amount of data can be occupied when comparing to the normal system which ultimately increases the capacity of the secrecy region by optimal utilisation of the same.

Next we are going to analyse the BER value, ie the bit error rate of the system. From the result it is found that BER value is very negligible such that it can be eliminated and considered as a zero value. The below given figure shows the graph plot for the BER value.

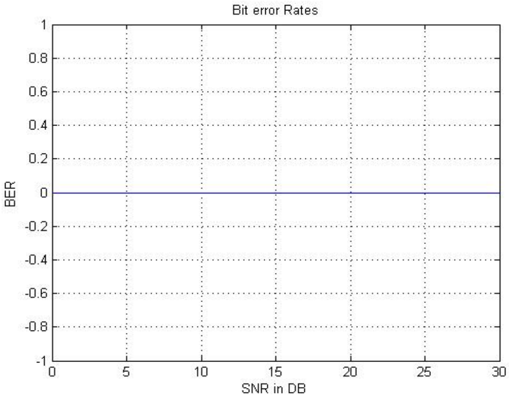

Fig.4.4 graph for BER

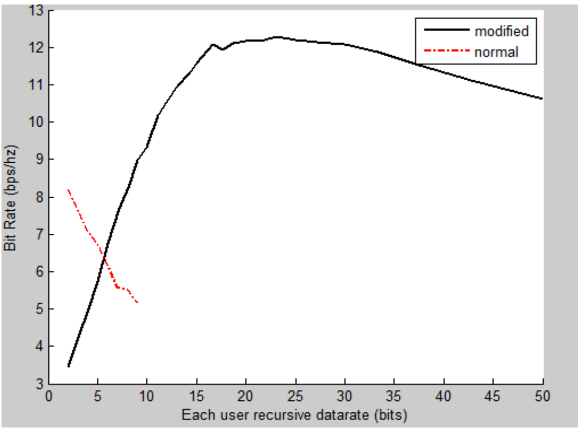

Fig4.5 transmission rate

The above given graph shows the transmission rate of the system. The line is given for the normal and the black line is representing modified system. From the graph itself it is shown that the modified system has more transmission rate when compared to existing.

In normal system when the data rate increases the bit rate reduces and reaches a small amount and finally to null point. Hence when transmitted for long distance it can lead to data loss. But in the modified system even though the data rate increases bit rate is more and it reaches the null point gradually. So we can transfer more data without loss.

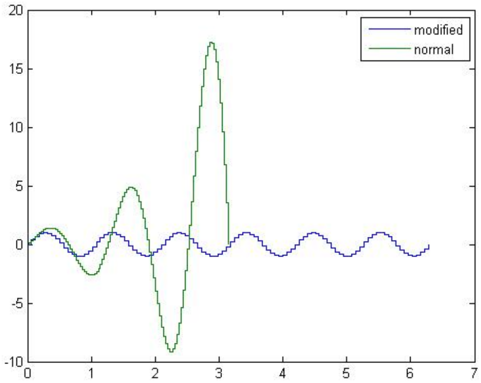

Fig.4.6 range comparison

In the figure green line represents the normal system and blue represents the modified system. In the modified system the data transmission will be normalised hence it can travel more distance without loss but in the normal system data loss occurs and hence it cannot travel more distance. So using the modified system we get more range when compared to the normal system.

Next we are going to compare the secrecy of the existing system with the modified system. Even when the eavesdroppers obtain some CSI information they cannot recover the data.

$$H_e=H_c+\sigma_e\delta$$

Here δ is mean squared estimation error. The eavesdroppers obtain H_e channel information which will be very different from the original CSI so they won't be able to attain the information or the data. Hence our system will be able to maintain secrecy.

V. CONCLUSION

In this paper we are proposing a precoder and postcoder design when the partial and the full CSI is known. With the help of this system we were able to increase the capacity of secrecy region,for this we uses modified Lloyds algorithm as precoder .We are using a postcoder for normalizing SNR value. From the analysis it is proved that this system provides secrecy and at the same time it provides good Bit error rate ,range and reliability when implemented in MIMO-OFDM systems

REFERENCES

[1] Chia-Hua Lin, Shang-Ho (Lawrence) Tsai, Senior Member, IEEE, and Yuan-Pei Lin, Senior Member, IEEE "Secure Transmission Using MIMO Precoding" IEEE transactions on information forensics and security, vol. 9, no. 5, may 2014

[2] A. Khisti and G. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[4] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 640–649, Sep. 2011.

[5] P. L. Yu and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 606–615, Sep. 2011.

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

[7] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in Proc. Military Commun. Conf., Nov. 2008, pp. 1–7.

[8] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress, Brazil, Rep. 42-44, 1978, pp. 114–116.

[9] H. Dinh, C. Moore, and A. Russell. (2010, Aug.). The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks [Online]. Available: http://arxiv.org/bs/1008.2390

[10] Z. Yang, C. Zhang, and L. Xie, "On Phase transition of compressed sensing in the complex domain," IEEE Signal Process. Lett., vol. 19, no. 1, pp. 47–50, Jan. 2012.

[11] A. D. Wyner, "The wire-tap channel," Bell. Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[12] I. Csis`zar and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348,May 1978.