ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2023.0264

AN INTENSE ANALYSIS OF OPTICAL WIRELESS MEDIUM TO IMPROVE THE SECURITY

E. Kamalanaban[1], R. Kannamma[2], G. Uma Maheswari[3] and M. Jayaprakash[4]

[1]*Department of Computer Science and Engineering, Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College, India*
[2]*Department of Artificial Intelligence and Data Science, Prathyusha Engineering College, India*
[3]*Department of Computer Science and Engineering, RMK college of Engineering and Technology, India*
[4]*Department of Information Technology, RMK Engineering College, India*

Abstract

This paper presents a numerical analysis of the performance of a multi user (MU) – Optical MIMO (OMIMO) system based on the uplink scheduling algorithm in optical wireless medium. The proposed approach makes use of the A antennas and the ZF multiuser detector located in the receiver, which makes it possible to choose U users from a pool of U_t>U users, who transmit at the same time to maximize the signal-to-noise ratio (SNR) of the shared radio resource they are accessing, in order to get the best possible reception. The performance of the proposed system is evaluated by making use of numerical findings that were obtained from Monte Carlo simulations that were carried out with $5x10^7$.

Keywords:

Wireless, Security, Optical, Signals, Channel

1. INTRODUCTION

The data that is transmitted over wireless networks is done so in a broadcast fashion, these networks are vulnerable to both passive and active forms of attack. Traditional cryptographic methods, such as the Diffie-Hellman key exchange [1] and the discrete logarithm [2], amongst a great number of others, require difficult mathematical computations, which an adversary may or may not be able to easily complete. This is due to the fact that the amount of time necessary to break the secret code can take longer than the time period during which the data is still accurate. In spite of this, the creation of quantum computers and the flurry of ongoing research in the field of quantum cryptography have increased the probability that the level of security afforded by such approaches may, in the not-too-distant future, be compromised. This is because quantum computers and quantum cryptography are both fields that rely heavily on quantum mechanics.

Conventional systems are not available for very much longer, which implies that an improved infrastructure for key management will be required in the near future. Quantum cryptography [3] is a method for securely sending information between nodes that does not rely on the use of a shared secret key but rather employs ideas from quantum theoretical models, such as Heisenberg uncertainty principle. This allows quantum cryptography to circumvent the security flaws associated with the usage of shared keys. Physical Layer Security (PLS) [4, 5, 6] or information-theoretic security has only lately emerged as a viable alternative to standard cryptographic systems, and related studies have only recently developed. Both of these developments occurred quite recently.

The idea of a system in which there is no ambient noise whatsoever is just a possibility in theory rather than in actual practice. In point of fact, the channel used by an eavesdropper may have a lower level of background noise compared to a genuine link, and the exchange of secret keys may entail major security problems. As a direct consequence of this, there is an immediate and compelling necessity to design measures for the protection of wireless networks. In a general sense, PLS approaches can be broken down into two categories: key-based schemes and key-less schemes, respectively.

The movement of the transmitter, the receiver, or other adjacent objects might add temporal variation into a channel. Spatial decorrelation assures that the channel between any two nodes is distinct, and an adversary who is positioned in a third location views an uncorrelated channel. Because it may be difficult for the adversary to obtain the channel state information (CSI), different keys may be generated for the legal pair and the adversary.

2. RECEIVED SIGNALS

According to what we can see, the uplink of this single-cell MU-OMIMO system looks like this: AU. This is due to the fact that the user terminals (UTs) each have one antenna, whereas the base station (BS) is outfitted with many $A \geq U$ antennas: .

When simultaneously broadcasting, U UTs use a frequency channel that is referred to as a subcarrier. This frequency channel has a bandwidth that is narrower than the channel coherence bandwidth, also known as *Bc*. Flat fading will have an impact on the signals that are being transmitted. This scenario occurs in multicarrier systems that use orthogonal frequency division multiplexing (OFDM), in which the entire bandwidth of the system is more than *Bc* while the bandwidth of each subcarrier is substantially lower than *Bc*. In other words, the total bandwidth of the system is greater than *Bc*. The subcarriers will be susceptible to flat fading as a result of the combination of this factor with the decrease in ISI and ICI that is accomplished by the employment of a cyclic prefix. It is possible to describe a symbol interval **y** with a length of $A \times 1$, which denotes the time period during which samples were received in the BS, as follows:

$$\mathbf{y}=\mathbf{H}\mathbf{s}+\mathbf{n}, \quad (1)$$

where **s** is a vector $U \times 1$ that represents the symbols that are being transferred and where these $A \times U$ symbols are being communicated. s_k is the symbol that is communicated by the k^{th} user, and $\mathbf{H}=[\mathbf{h}_1, \mathbf{h}_2 \cdots \mathbf{h}_U]$ is an AU matrix that reflects the gains of the wireless channels. $\mathbf{h}_k$ is the symbol that is conveyed by the user. As a consequence of this, the A channel gains that have an impact on the transmission of the k^{th} user can be located in the $\mathbf{h}_k$ column vector of the matrix. $\alpha_{a,k}$ is the fading amplitude modeled by a Rician random variable, whose PDF is defined by

$$h_{a,k}=g_1+jg_2$$

where g_1 and g_2 are real Gaussian random variables with a mean and a variance, and $h_{a,k}=\alpha_{a,k}\exp(j_{\phi a},k)$ is a vector of complex Gaussian random variables. The channel gains when the fading amplitude is represented by a Rician random variable whose PDF is defined by k=1,2,...,U and a=1,2,...,A, respectively. The channel gains may be computed with a higher degree of precision.

$$f_\alpha(\alpha)=\frac{2(K+1)}{P}\alpha I_0\left(2\alpha\sqrt{\frac{K(K+1)}{P}}\right)\exp\left(-\frac{K+1}{P}\alpha^2-K\right) \quad (2)$$

where

$I_0(\cdot)$ - Bessel function, and

$$K=\mu_{22}/\sigma^2, \quad (3)$$

where,

μ_{22} - shape parameter and

K - ratio of the LOS power and the non-LOS power along the path of transmission.

$$P=\mu^2+2\sigma^2, \quad (4)$$

where

P - power received.

$\phi a,k$ - channel phase.

It is possible to determine the marginal PDF of by using the joint distribution of α and ϕ. This will allow for the determination of the marginal PDF ϕ:

$$f_\Phi(\alpha)=\int_0^\infty f(\alpha,\Phi)\,d\alpha \quad (5)$$

where erfc(·) - error function.

To show that we are not to be outdone, here is is the AWGN vector, and its components are complex Gaussian random variables with zero mean and variance ($\sigma^2 n$), or CN(0,$\sigma^2 n$), where $\sigma^2 n=N_0/(2T_s)$ is the noise variance, N_0 is the unilateral noise power spectral density, and T_s is the symbol time. The AWGN vector is a complex Gaussian random variable with zero mean and variance.

2.1 MALMQUIST MODEL

Prior calculating the DEA efficiencies, it is important to first ascertain the connection between input and output. This must be done before the DEA efficiencies can be calculated. It has been settled that an investigation utilizing Pearson correlation would be carried out. In empirical research, the coefficient that is named after Bravais is called the Pearson coefficient.

The correlation score for each pair of components or data sets indicates, on a linear scale, the degree to which two components or data sets are reliant on one another. This score compares the two components or data sets in question. When two variables travel in the same direction at the same time, this is an example of a positive correlation; on the other hand, this is an example of a negative correlation, which occurs when one variable goes in the opposite direction while the other variable moves in the same way.

The correlation coefficient has a range of possible values that goes from -1 all the way up to +1. Two distinct collections of information are said to have a linear relationship between them when the correlation coefficient is relatively close to +1 or 0. For the purpose of determining a Pearson's correlation coefficient:

$$r_{xy}=\frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})\sum_{i=1}^{n}(y_i-\bar{y})}} \quad (6)$$

3. SCHEDULING ALGORITHM USING FROBENIUS NORM

The most recent research takes into account the possibility that some user terminals do not have certain features installed on antenna A_u, and the fact that the base station makes use of receiving antennas means that it gives precedence to the user who is sending the greatest channel energy.

$$u_0=\text{argmax}_k\|\mathbf{H}_k\|^{2F},\ k\in\{1,2,\ldots,U_t\} \quad (7)$$

where

U_t - users that are sharing the available bandwidth $U_t \geq U$ and

$\mathbf{H}_k$ - $A\times A_u$ matrix that represents the channel gains of the k^{th} user (in order to preserve consistency with the proposed system model, Au=1).

The algorithm moves on to the subsequent user who is accountable for the largest contribution to the total equivalent aggregate channel energy among the selected users.

$$u_i=\text{argmax}_{k\in\Psi}\sum\|\mathbf{H}_{\text{eq}}{}^{\ell}\|\|^2{}_F, \quad (14)$$

where Y and Ψ - participation and the users that has not yet made a choice. In order to produce an equivalent channel matrix, the initial channel matrix is multiplied by a precoding matrix. This results in the production of the equivalent channel matrix $\mathbf{H}_{eq}{}^{\ell}$, which can be modeled using Equation.

The system finds out which of the available options the user chooses to go with during the second encounter. After U users have been chosen, the algorithm is finished and the result u_i is displayed. When taking into account the fact that Au=1, this method is able to carry out different complex operations, including complex additions and complex multiplications, amongst others.

Under these conditions, the amount of computation time necessitated by the proposed algorithm could very well be quite substantial. For this reason, the system has to have the capability of selecting an acceptable value of U_t based on the number of users that can be serviced by each radio resource (U), as well as the processing power of the receiver.

The system needs to be able to select an acceptable value of U_t based on the number of users that can be serviced by each radio resource. Even though there are multiple radio resources that are accessible within each cell, the fact that a mobile network can support a large number of users within a single cell does not necessarily mean that all of these users are competing with one another to broadcast. This is the case even though the mobile network is able to support a large number of users.

The BS is in a position to be able to make an informed decision regarding the value of U_t based on the characteristics of its own processing capabilities as well as the operating parameters of the system. This enables the BS to minimize the risk of making an

incorrect estimate of the value of U_t. However, it is essential to keep in mind that this only applies to systems that are operating at their utmost capacity. It is that it will be used in circumstances in which the difference between U_t and U is sufficiently negligible so that the output of operations generated by the scheduling algorithm.

4. NUMERICAL RESULTS AND DISCUSSION

In this section, the efficiency of the proposed system is evaluated by making use of the numerical findings that were obtained from Monte Carlo simulations that were carried out with 5×10^7. During the course of the testing, a selection of typical use cases are utilized, and various settings were used for the critical operating parameters. Matlab® is utilized in the process of arriving at these numerical results.

The simulations are done under the assumption that the BS has A antennas and serves U users, and that the symbols that are being transmitted are a part of a constellation with normalized mean power, which is denoted by $E[s_k^2]=1$. In a wireless system that does not have ICI or ISI, also known as flat fading, it is assumed that all users are broadcasting at the same time on the same frequency subcarrier. Another assumption that we have made is this one.

In the event that Rician fading has a value of $2\sigma^2=1$, we can derive from equation 3 that the mean power of the multipath has been normalized. This can be done by assuming that Rician fading has this value. The performance of the OMIMO system is evaluated based on its OP, BER, and SOP, with the presence of a spy receiver being taken into consideration for the evaluation of the SOP. The multiple figure captions that are displayed provide a more in-depth breakdown of the simulation settings than is previously presented.

According to the findings, an increase in AE also leads to an increase in OP. This is something that can be seen in the statistics. This is because the eavesdropper, as a result of its rising variety, is better able to decode the information that the users are providing.

This is due to the fact that the diversity of the eavesdropper is increasing. In addition to this, it can be seen that the OP curves seem to have a floor that does not get lower when the Eb/N0 ratio gets higher.

The trustworthy BS and the eavesdropper benefit from an increase in the Eb/N0 ratio since it correlates with an increase in the transmission power of the user terminals. This is because the increase in Ut has a multiplicative effect. Because U_t and U are equal, the scheduling process is not carried out when the value of U_t = 3. On the other hand, scheduling is carried out whenever U_t = 5, which raises the OMIMO system level of dependability.

As a result of an increase in the average power of the fading channel for pathways between the eavesdropper and the UTs, the SOP grows in proportion to the value of c as a direct consequence of the increase in power. It is simpler for an eavesdropper to decipher the data that is being sent by the users of the system.

The overall SOP is decreasing in U_t that has been implemented. The proposed approach of scheduling makes it feasible to attain the best possible SNR for the chosen group of transmitting users whenever U_t is at its highest. This is made possible thanks to the fact that the system takes into account user preferences. This leads to an increase in the UT attainable rate suggests a lower SOP.

Table.1. Optical Wireless Medium (SOP) in robust conditions with 10 users

Optical Wireless Medium	Rician Fading	Rayleigh Fading	Rician Fading with U users	Rayleigh Fading with U users
2	5.66	5.23	5.02	4.85
4	6.52	6.01	5.83	5.62
5	7.84	7.22	6.98	6.67
6	8.92	8.62	8.32	8.01
10	9.95	9.55	9.21	8.62

Table.2. Optical Wireless Medium (SOP) in robust conditions with 20 users

Optical Wireless Medium	Rician Fading	Rayleigh Fading	Rician Fading with U users	Rayleigh Fading with U users
2	3.32	3.07	3.01	2.91
4	4.00	3.70	3.65	3.42
5	5.06	4.66	4.57	4.32
6	5.92	5.78	5.64	5.33
10	6.74	6.52	6.35	5.95

It is evident that the SOP values shown in Table.1 are lower than those shown in Table.2. This is a result that the reliable BS uses two antennas, but the eavesdropper only uses one antenna to transmit and receive signals. It is found that a growing U_t leads to a decreasing SOP. These findings provide proof that it is possible to obtain an enhanced FN for OMIMO systems with the support of the scheduling algorithm and several other methods.

The findings show that it is possible to achieve an improved PLS for OMIMO systems. Because user selection is based on the channel status information that is shared between the UTs and the BS, it is important to note that the eavesdropper does not have any way of knowing which users are transmitting. This is because the information is shared between the UTs and the BS. Users using the OMIMO system are afforded a greater degree of flexibility with regard to the method in which they transmit private information.

5. CONCLUSION

The uplink scheduling approach makes main use of the A antennas and the ZF multi-user detector located in the receiver. Both of these components are used in the receiver. The proposed solution gives the system the capacity to choose U users from a pool of $U_t>U$ users, who transmit at the same time to maximize the SNR of the shared radio resource they are accessing in order to get the best possible reception.

The number of complicated operations is counted in order to estimate the computational complexity of the approach that is recommended. It is found that both the OP and the BER decrease

with increasing U_t, which means that the technique that is advocated improves the performance of MU-OMIMO systems. In addition to this, it is discovered that a higher level of system diversity is attained with U_t values that were greater. Interference is eliminated, and diversity is increased, even when the system is completely loaded.

In addition, the findings indicate that the strategy that is proposed reduces the negative effects that are the direct result of channel estimation mistakes, and that this reduction is made more effective as U_t increases. The technique that is proposed makes it possible to maximize the SNR of the users, which in turn makes it possible to raise the rate that the users are capable of achieving, which in turn makes it possible to reduce the SOP of the MU-OMIMO system in a situation in which an eavesdropper is present.

REFERENCES

[1] S.A.H. Mohsan and H. Amjad, "A Survey of Optical Wireless Technologies: Practical Considerations, Impairments, Security Issues and Future Research Directions", *Optical and Quantum Electronics*, Vol. 54, No. 3, pp. 187-197, 2022.

[2] I.S. Amiri and J. Ali, "Review and Theory of Optical Soliton Generation used to Improve the Security and High Capacity of MRR and NRR Passive Systems", *Journal of Computational and Theoretical Nanoscience*, Vol. 11, No. 9, pp. 1875-1886, 2014.

[3] S.A.H. Mohsan and H. Amjad, "Hybrid FSO/RF networks: A Review of Practical Constraints, Applications and Challenges", *Optical Switching and Networking*, Vol. 87, pp. 100697-100707, 2022.

[4] L. Xiao and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels", *IEEE Transactions on Wireless Communications*, Vol. 7, No. 7, pp. 2571-2579, 2008.

[5] V.A. Memos, B.G. Kim and B.B. Gupta, "An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework", *Future Generation Computer Systems*, Vol. 83, pp. 619-628, 2018.

[6] F.A. Alaba and F. Alotaibi, "Internet of Things Security: A Survey", *Journal of Network and Computer Applications*, Vol. 88, pp. 10-28, 2017.

[7] Z. Ghassemlooy, S. Arnon and J. Cheng, "Emerging Optical Wireless Communications-Advances and Challenges", *IEEE Journal on Selected Areas in Communications*, Vol. 33, No. 9, pp. 1738-1749, 2015.

[8] A.C. Boucouvalas and K. Yiannopoulos, "Standards for Indoor Optical Wireless Communications", *IEEE Communications Magazine*, Vol. 53, No. 3, pp. 24-31, 2015.

[9] R. Tang and Y. Han, "High Security OFDM-PON based on an Iterative Cascading Chaotic Model and 4-D Joint Encryption", *Optics Communications*, Vol. 495, pp. 127055-127067, 2021.

[10] K. Pelechrinis and S.V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers", *IEEE Communications Surveys and Tutorials*, Vol. 13, No. 2, pp. 245-257, 2010.