Abstract: Physical layer data communication and security under the channel has become a raising concern for communication researchers. Under VLC the high level privacy and security updating policies are informed and moderated. The overall paper focuses on various modulation and demodulation approaches in preserving the identity of the bits and security of the transmitting data.

Index Terms — Visible Light Communication (VLC), Light-Emitting-Diode (LED), Fields of View (FoV), Multi User (MU).

I. INTRODUCTION

Visible light communication (VLC) is an emerging technology for short range wireless networking that can offer energy efficient data streaming through lighting system. Visible spectrum covers wave lengths from 380 nm to 750nm. VLC or Light-Fidelity (Li-Fi) is IEEE 802.15.7 standard released on 2011. VLC systems benefit from an unlicensed spectrum, immunity to radio frequency (RF) interference, and the use of inexpensive LEDs and photodiodes for modulation and demodulation, respectively. Due to line-of-sight propagation and confinement of light waves by opaque surfaces, VLC networks cooperate coverage and mobility for improved security and compact internetwork interference. Such advantages tend VLC take to small size cells called as ‘atto-cells’ which is used in fifth generation (5G) networks with coverage ranges on few meters.

Physical-layer security refers to the techniques which exploit the channel characteristics in order to hide information from unauthorized receivers, without reliance on upper-layer encryption. The fundamental idea behind physical-layer security is to sacrifice a fraction of the communication rate, that otherwise would be used for data transmission, in order to confuse potential eavesdroppers and diminish their capability to infer information, via carefully designed signaling and/or coding schemes the visible light communication (VLC) refers to the communication technology which utilizes the visible light source as a signal transmitter, the air as a transmission medium, and the appropriate photodiode as a signal receiving component.

II. BACK GROUND WORK

Multiple papers have referred as part of this literature review and arrived at the following details: The physical-layer security techniques can be used to enhance the confidentiality of VLC links. The Visible Light Communication scenario consists of a transmitter, a legitimate receiver and an eavesdropper. Ayman Mostafa et al. [1] mathematically derived closed-form lower and upper bounds on the secrecy capacity of the amplitude-constrained wiretap channel. The achievable secrecy rates for the MISO channel and zero-forcing is obtained using the beam forming technique and is an appropriate strategy for secure transmission over MISO VLC channels and proposed a practical robust beam forming scheme which considerably improves worst-case secrecy rates.

The challenge is that robust beam forming functionality will be effective only when the position of the Eve is known [1]. Yang Hong, Jian Chen, Zixiong Wang [2] investigated BER and SNR performances of the proposed precoding MIMO indoor VLC system for decentralized multi-user. By using block diagonalization (BD) precoding algorithm the multiuser interference is eliminated in transmitter. It reduces the power consumption and complexity of user terminals. A method to improve the system performance by utilizing different field of view (FOV) is analyzed. A high SNR communication channel up to 40 dB is achieved through simulation results. When the single LED’s power exceeds 10 mW, the system can achieve 100 Mbit/s at a BER of 106 while 70 deg and 50 deg are adopted as FOVs for the optical receivers which belong to single user terminal.

High brightness LED is the main component of this communication system, which acts as a communication source and a photodiode which shows good response to visible wavelength region serving as the receiving element. Digital strings of 1s and 0s are generated by switching the LED on and off. By varying the flickering rate of the LED, data can be encoded in the light to generate a new data stream. The LED get illuminated when one dc bias is included. So by modulating the LED light with the data signal, the LED illumination can be
used as a communication source. The LED output appears constant to the human eye, since the flickering rate is so fast. High speed LEDs can produce a data rate of greater than 100Mbps by using with appropriate multiplexing techniques. Using LED arrays VLC data rate can be increased by parallel data transmission where each LED transmits a different data stream. The receiver uses photodiode for down conversion of the signals. Photodiode is a semiconductor device that converts light into current by using photoelectric effect and analyze the data using both software and hardware.

III. SYSTEM IMPLEMENTATION

The proposed system is implemented on identifying the system components under VLC resource utilization. The system block diagram is shown below in fig 1.

**Fig 1: Proposed system block diagram**

In this is a tentative block diagram derived from my base paper, here initially I collect the samples and sense using the photonic sensors under a simulative environment. On receiving the data, Data modulation techniques is been appended for single wavelength value calibration. These messages under an authentic channel of VLC is been transmitted under transmission unit / channel.

The system is demonstrated with a block diagram shown in Fig 1. basically the system consist of a primary data acquisition unit for sample data collection from LED and thus a threshold stream of data for a monitored space is been sent. The acquired data streams are robust and are reconfigured manually under MATLAB simulation cum coding environment.

On receiving a data from LED’s, the modulation technique is initiated and data streams are proceed under the following approach. The modulation includes a physical layer, serial to parallel bit modulation. Data bits transfer on this modulatory channel to support a higher security and data reliability for sharing. The demodulation technique at the receiver captures the data segment bits and thus demodulates under the inverse operation of this. The demodulated code is future analyzed and decoded under last unit. This unit demonstrates the redundancy of bit elimination under ambiguous conditions.

The data is inserted via a manual interaction in environment of processing; the data bits are independent and are aligned as per the scenarios. Fig 3 demonstrates the overall modulation performed under our proposed system.

**Fig 2: MISO input Data Streams**

**Fig 3: Data Modulation**

**Fig 4: Data Demodulation**

**Fig 5: BER Computation for proposed system**
In the figure 3, the data modulation under system scenario of modulation and demodulation is shown, the input data is supposed to be secure and reliable and hence it is compared and generated a BER value graph for the overall input streams. The system is efficient and hence produces the efficient flow on BER under normal and appended parametrics.

IV. CONCLUSION

The paper has focused on random input stream processing of data bits under a normal and hyperactive channel of modulation techniques. These techniques are correlated and are inter divergent for modulation effect, the overall resultant is acquired and is simulated for the above shown diagram. The resultant BER values and ratios are demonstrated and shown in the paper.

REFERENCES


