Beam Scanning based Secure Communication using Visible Light

Muhammad Saadi, Ali Nasir

***Abstract* – Recent advancements in wireless communication provides an opportunity to connect to the internet without wires but at the cost of risks associated with data integrity and confidentiality. With the unprecedented growth of wireless applications, the security concerns in wireless communication are also touching the skies. In this paper, a novel approach has been presented which establishes a secure communication link using optical wireless communication. Secure transmission is attained by first scanning of beams of spatial diverse transmitters and then establishing the connection based on the feedback received from the receiver. For the downlink, we have used visible light a spectrum for communication and for uplink Infrared (IR) is used to avoid spectrum interference and visual inconvenience. A detailed investigation has been carried out for various step size (position) of the transmitters and its effect on shrinking the room area. Experimental results demonstrate that a secure communication link can be established using the proposed approach with less probability of interception when compared with conventional transmitters.**

***Index Terms* – light emitting diodes, secure communication, optical wireless communication**

I. INTRODUCTION

Bandwidth hungry applications has invigorated the researchers to discover new ways of telecommunication. Visible light communication (VLC) which is a part of optical wireless communication (OWC) is one of the promising technology which has the potential to fulfill the emerging needs of bandwidth and ensures environmental friendliness [1]. With recent advancements in solid state lighting (SSL), VLC have provided a unique opportunity to realize low cost, hazard free, high speed, energy efficient and secure wireless communication in conjunction to lighting [2]. LEDs offer many advantages over conventional and florescent lighting such as high tolerance to humidity, prolonged mean time before failure (MTBF), low power consumption, mercury free etc.

Radio frequency (RF) communication spectrum is not only getting congested but also suffers from its open nature of RF propagation which give rise to significant security threat. However, as light cannot pass through the concrete structure so it gives an in-built security thus reducing the chances of eavesdropping, traffic analysis, resource consumption, message modification, masquerade attacks and hacking [3]. An un-intercepted secure transmission of confidential information only to the intended user(s) is crucial in modern information and communication era. To maintain the data integrity, classical network cryptography techniques are being widely used at upper layers of wireless networks, however, in future, the wireless networks will be decentralized and massive in scale which can thus increase the computational complexity for cryptographic techniques [4]. Furthermore, there is a probability that attackers can decrypt the encrypted confidential information.

Other than the cryptographic techniques, there exists physical layer secure approaches as well which can be classified into five categories namely, theoretical secure capacity, channel approaches, power approaches, code approaches and signal design approaches [5]. Using theoretical secure capacity approach, a system can be designed to achieve definite degree of secrecy but not the absolute one. Furthermore, this technique requires the knowledge of communication channel which might not be precisely available for all practical communication channels [6]. The channel approaches for attaining security is capture and extract electromagnetic wave features of the received signal with the help of multiple sensors or through transmitted code vectors. One popular method in channel approaches in randomization of multiple input multiple output (MIMO) transmission coefficients thus making the matrix undetectable to the intruder [7]. The third physical layer approach for data protection is the power approach in which directional antennas are used [8]. Other than that, artificial noise schemes can be introduced which makes intruder channel nosier than the intended receiver [9]. The code approaches are primarily used for anti-jamming and to avoid eavesdropping by employing spread spectrum or error correction codes [10]. A recent approach utilizing visible light for secure communication is through 2D barcode scanning which can be used as an alternative to near field communication technologies [11].

Inspired from the concept of multiple antennas for secure wireless communication, a proper space-time diversity at the transmitter can help enhancing the information confidentiality [3], [12], in this paper, we propose a novel technique for secure data transmission at physical layer. Two transmitters are used for transmission the data instead of one. The receiver will only be able to reconstruct the transmitted data if it can receive data from both LEDs and the complete description and implementation details are mentioned in Section 2. Section 3 talks about the design of transmitter and receiver. Section 4 discusses the results of the proposed approach and how communication can be made secure. The paper is concluded in Section 5.

II. PROPOSED SCHEME

The proposed technique can be classified as a hybrid approach of theoretical secure capacity and power approach. In order to bring robustness to our system so that the probability of interception, probability of detection and probability of exploitation, the proposed technique consists

Muhammad Saadi and Ali Nasir are with Department of Electrical Engineering, Faculty of Engineering, University of Central Punjab, Lahore, Pakistan. Email: muhammad.saadi@ucp.edu.pk, a.nasir@ucp.edu.pk.
Manuscript received on Jul 05, 2017 revised on Oct 11, 2017 and accepted on Dec 20, 2017.

ISSN – 1999-4974

of two transmitters and a receivers. These transmitters consists of stepper motor along with its driving circuit and LED along with its driving circuit. The receiver consists of not only the photodiode but also an Infrared (IR) LED array which is responsible for transmitting the feedback signal from the photodiode to the LED transmitters. Thus the proposed scheme is establishing a full duplex channel for secure communication. The proposed technique for secure communication consists of the following steps

A. *Beam Scanning and Position Locking*

The transmitter consists of two LEDs. These LEDs are placed at the corners of the room These LEDs are made to move so that it can cover the whole area of interest. The LEDs are pointed downwards facing the area with the elevation angle of $\theta_{e,i}$. The beam emitted with $\theta_{e,i}$ will have its projection in a conical geometry on 2D plane and its vertex is defined as a location of a virtual point source Each transmitter will be moved in six steps and its position will be locked based on the acknowledgement signal from the receiver when the receiver is receiving the maximum signal strength. By doing so, the receiver will be receiving the strongest signal from both transmitters depending upon the location. The described scenario is shown in Fig. 1.

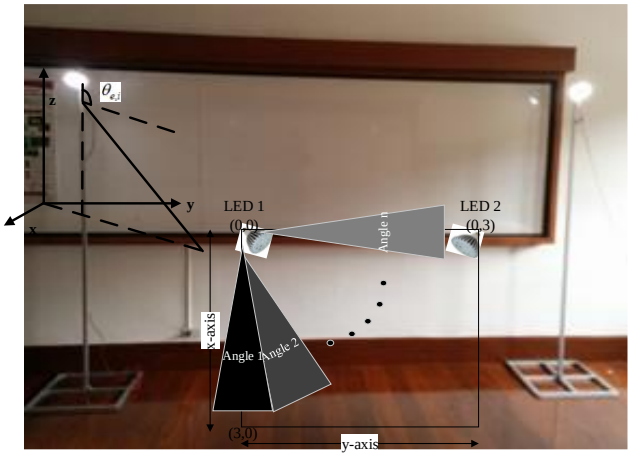

Fig. 1 Scanning the beam to transmit maximum signal strength from the receiver

B. *Data Splitting and Transmission*

After this handshaking process, the communication between the transmitter and the receiver initiates. The information which need to be transmitted is divided into two halves, one is fed to *I* transmitter and the remaining is fed to *Q* transmitter. So the next of the proposed secure communication is the splitting of the data into *I* and *Q*.

C. *Data Reception and Noise Filtration*

The purpose of beam scanning and data splitting was to make the communication secure. The receivers can be anywhere in the area of interest, however, when beam scanning is done then the intended receiver location is known and beams at directed towards that side only. If the malicious receiver is the region where only one channel is being transmitted then that receiver will not be able to recover the complete information. So, any other receiver which is not the in joint footprints of *I* and *Q* LEDs, will not be able to recover the transmitted signal completely. This process will help reducing the probability of interception.

D. *Data Recombination*

The last step is to combine both *I* and *Q* channel transmission and form a composite received signal. Then the signal can be fed to any further processing.

The complete theme of the concept can be visualized in Fig. 2.

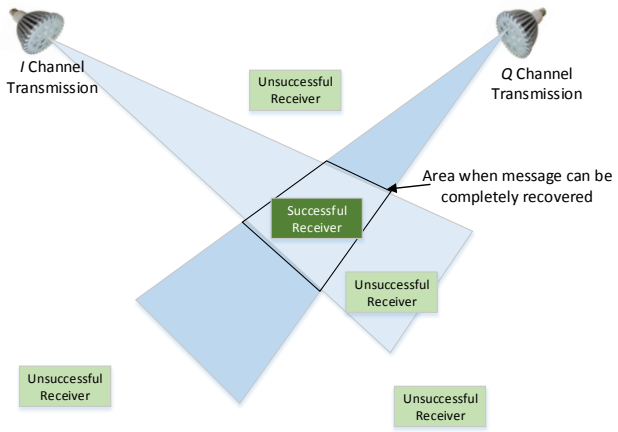

Fig 2. Secure communication using diversity based transmission

III. TRANSMITTER AND RECEIVER DESIGN

In this section, the design of transmitter and the receiver is discussed. The transmitter consists of quadrature generator which is responsible for generating sine wave and cosine wave.LT1260 is used as quadrature generator and it is tuned with the help of resistors and capacitors to get the desired frequency output. Each sinusoidal wave is fed to the multiplier and the second input to the multiplier is the output of the data splitting which is done is Arduino microcontroller. Signal is amplified to an appropriate level which then becomes suitable for transmitting the signal to the channel with the help of LED driver circuit and the LEDs. The transmitter block diagram is shown in Fig. 3.

Signal from the channel will be received by the photodiode which produces a proportional current with respect to the intensity of the light. Due to channel degradations, the signal will be weak so trans-impedance amplifier (TIA) is used. The output of TIA will be fed to the differential amplifier for adaptive minimum voltage cancellation (AMVC) which will remove the effect of ambient light noise from the received signal. The block diagram of the receiver is shown in Fig. 4.

IV. RESULTS AND DISCUSSION

The transmitted signal from both channels will go through the channel and reach at the receiver. Noise will be introduced by the channel in the signal. For our experiment, we have placed our setup not under direct sun light and the experiment is performed under moderate lighting condition.

ISSN – 1999-4974

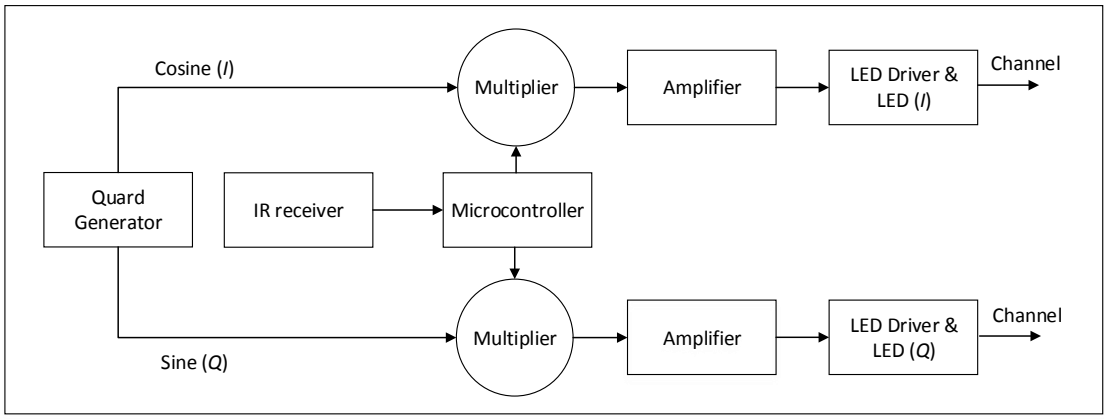

Fig. 3 Block diagram of transmitter

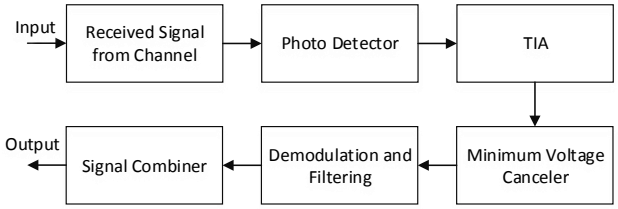

Fig. 4 Block diagram of the receiver

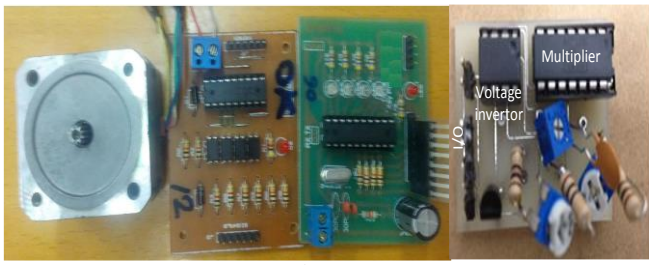

Fig. 5 Motor control unit (left side), transmitter module (right side)

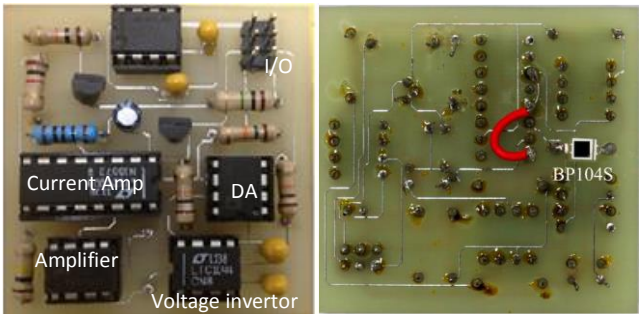

Fig. 6 Receiver's module front side (left), back side (right)

The advantage of controlled lighting system is less noise contributed from the channel.

As mentioned earlier, when the signal will go to the channel, noise will be added to the signal and the photodiode will be received a combined signal which contains both *I* and *Q* signal and is shown in Fig. 7.

After the reception of the signal, next is to demodulate the signal and to perform filtering. The demodulation can be done by multiplying the received signal with the local carrier of the same frequency as that of I channel and *Q* channel. Multiplying the received signal with *I* channel local oscillator will lead the data of the *I* signal and multiplying the received signal with the *Q* channel local oscillator will retrieve the data from the *Q* signal. After demodulation, the signal is then passed through the low pass filter in order to minimize the effect of noise. After filtering, Inverse Discrete Fourier Transform (IDFT) is computed and the resulting signal is plotted in Fig. 8.

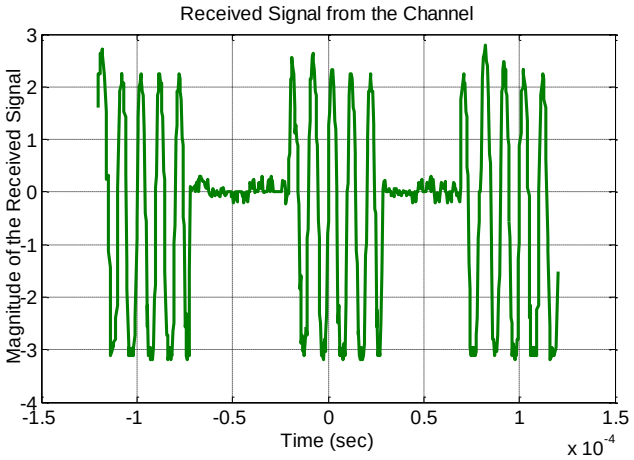

Fig. 7 *I* and *Q* signal received by photodiode

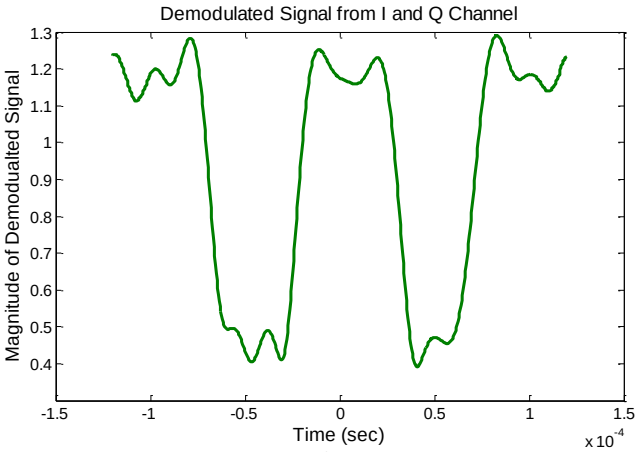

Fig. 8 Demodulated and filtered signal at the receiver

ISSN – 1999-4974

From Fig. 8, we can clearly see that the signal can be easily distinguished between low and high values and simple threshold detection scheme can be applied in order to obtain the binary data. This shows the proof of the concept that the spatially diverse transmitted signal using visible light can be recovered at the receiver by applying few well known techniques.

Suppose, in beam scanning phase, the position of transmitter 1 can be locked in n ways (i.e. number of sweeps LED can take from its origin position till final position). Similarly, assume that the position of transmitter 2 can be locked in m ways (where n and m can be equal but both should be equal to greater than 1). The number of intersecting points of both beams will be $n \times m$. In actual, each intersecting point will correspond to intersecting area and centroid of that area can be classified as an intersecting point. Let us assume that the consecutive sweeps of each LED beam doesn't overlap then we can calculate the area where successful communication can be established and thus estimate the probability of interception.

$$Area_{trans\_success} = \frac{Area_{total}}{n \times m} \quad (1)$$

Thus by doing so, we are shrinking the area where successful transmission can occur thus making it less probable for the intruder to intercept the communication despite the intruder is in the same vicinity. The overlapping area of the intersecting beams might not always be a perfect square or rectangle in shape, however, for the sake of simplicity, we can assume to be in square or rectangle in shape. In order to visualize the effect how room can be partitioned between secure communication area and non-secure communication area, plots have been drawn in Fig. 9. From the Fig. 9, we can clearly see as the number of transmitter increases, the secure area is confined to a small area and non-secure area in contrast in increasing exponentially.

If we consider a room of size 5×5 m^2 we can clearly see (in Fig. 10) if the number of steps (each transmitter can move) increases, then the area where confidential information can be intercepted is reduced. The green colored area in Fig. 10 shows the area where the receiver is receiving both the I and Q channel signals and for all other locations (white area), either one or none signal is received which means that the signal cannot be constructed perfectly.

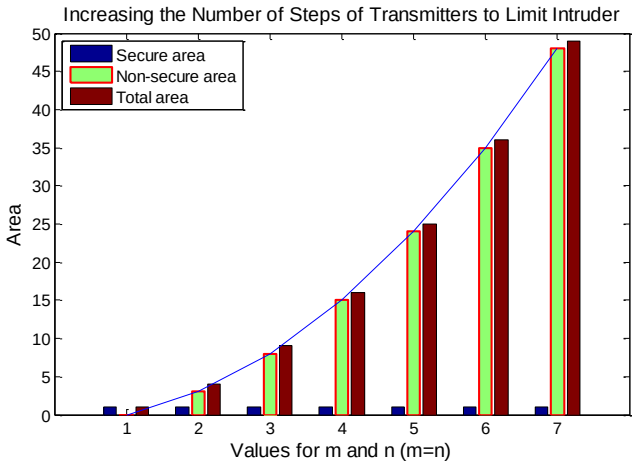

Fig. 9 Comparison on how the area is shrunk for secure communication with respect to non-secure area. Even if the intruder is the vicinity, still it is less probably to extract the information.

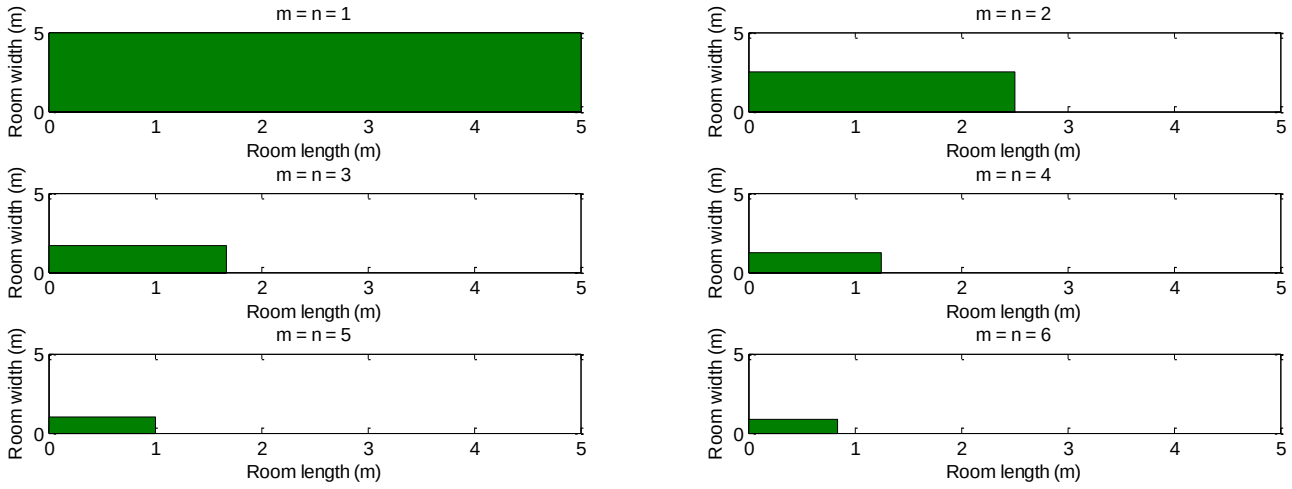

Fig 10 Reduction in the area where interception can take place as the step size increases.

V. CONCLUSION

In this paper, a novel method of establishing a secure communication link using optical wireless communication (OWC) has been demonstrated. We used two transmitters to broadcast the information with each transmitting partial information. In order for the receiver to receive the whole information, it must be in an area when beams from the both transmitters intersects. It is not convenient and practical for the receiver to move in an intersected area, therefore, a beam

ISSN – 1999-4974

scanning approach at the transmitter end is adopted in order to identify and validate the receiver. Such system are very desirable where confidentially and integrity of the data must be maintained. Our results show that a secure communication link can be achieved using the proposed approach with reduced probability of interception. Our secure communication approach can be classified as a hybrid approach of theoretical secure capacity and power approach as it employs space-time diversity as well as directionality.

REFERENCES

[1] Elgala, H., Mesleh, R. and Haas, H., 2011. Indoor optical wireless communication: potential and state-of-the-art. IEEE Communications Magazine, 49(9).

[2] Saadi, M., Zhao, Y., Naseer, O. and Wuttisittikulkij, L., 2016. A beam scanning-based indoor localization system using light emitting diodes. Engineering Journal (Eng. J.), 20(3), pp.197-206.

[3] Noonpakdee, W., Liu, J. and Shimamoto, S., 2011. Position-based diversity transmission scheme employing optical wireless communication. IEEE Transactions on Consumer Electronics, 57(3).

[4] Liu, R., Luan, L. and Xiao, G., Kuang-Chi Innovative Technology Ltd, 2017. Visible-light communication-based encryption, decryption and encryption/decryption method and system. U.S. Patent 9,768,958.

[5] Shiu, Y.S., Chang, S.Y., Wu, H.C., Huang, S.C.H. and Chen, H.H., 2011. Physical layer security in wireless networks: A tutorial. IEEE wireless Communications, 18(2).

[6] Nafea, M. and Yener, A., 2017. Secure degrees of freedom for the MIMO wire-tap channel with a multi-antenna cooperative jammer. IEEE Transactions on Information Theory, 63(11), pp.7420-7441.

[7] Mostafa, A. and Lampe, L., 2015, July. Enhancing the security of VLC links: Physical-layer approaches. In Summer Topicals Meeting Series (SUM), 2015 (pp. 39-40). IEEE.

[8] Zhou, X., Ganti, R.K. and Andrews, J.G., 2011. Secure wireless network connectivity with multi-antenna transmission. IEEE Transactions on Wireless Communications, 10(2), pp.425-430.

[9] Goel, S. and Negi, R., 2008. Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 7(6).

[10] Qin, L., Zhang, Y., Song, K., Li, B. and Du, Y., 2017. Visible light communication system based on spread spectrum technology for intelligent transportation. Optical and Quantum Electronics, 49(7), p.252.

[11] Zhang, B., Ren, K., Xing, G., Fu, X. and Wang, C., 2016. SBVLC: Secure barcode-based visible light communication for smartphones. IEEE Transactions on Mobile Computing, 15(2), pp.432-446.

[12] Saadi, M., Bajpai, A., Zhao, Y., Sangwongngam, P. and Wuttisittikulkij, L., 2014. Design and implementation of secure and reliable communication using optical wireless communication. Frequenz, 68(11-12), pp.501-509.

ISSN – 1999-4974