Design and Implementation of Secure and Reliable Communication using Optical Wireless Communication

Abstract: Wireless networking intensify the tractability in the home and office environment to connect the internet without wires but at the cost of risks associated with stealing the data or threat of loading malicious code with the intention of harming the network. In this paper, we proposed a novel method of establishing a secure and reliable communication link using optical wireless communication (OWC). For security, spatial diversity based transmission using two optical transmitters is used and the reliability in the link is achieved by a newly proposed method for the construction of structured parity check matrix for binary Low Density Parity Check (LDPC) codes. Experimental results show that a successful secure and reliable link between the transmitter and the receiver can be achieved by using the proposed novel technique.

Keywords: optical wireless communication, security, low density parity check codes, light emitting diode

PACS® (2010). 42.79.-e, 42.15.Eq

DOI 10.1515/freq-2014-0027
Received February 24, 2014.

1 Introduction

In recent years, demand for bandwidth demanding applications in mobile communications has been observed in addition to the exponential growth in the number of users. RF based technologies have spectrum congestion, interference, expensive licensing and high installation cost issues [1]. To overcome the above mentioned issues, an optical wireless communication (OWC) which uses optical radiations to convey information in air or free space can be used in conjunction or alternative to RF [2]. Visible Light Communication (VLC) refers to short range OWC which utilizes a human visible spectrum ranging from 380 nm to 780 nm [3]. The Visible Light Communication Consortium (VLCC) is the pioneers in VLC technology and in this area significant interest have been witnessed around the globe. This led to the formation of IEEE study group of VLC standardization and the standard was released in September 2011 [4]. With nearly 300 THz huge, unregulated, and unlicensed bandwidth available for VLC, multi gigabit/sec data rates can be achieved for a small range using LEDs [5–6].

Wireless networking intensifies the tractability in home and office environments to connect the Internet without wires. This luxury is attained at the cost of risks associated with stealing the data or threat of loading malicious code with the intention of harming the network. Implementation of security protocols can reduce the threat to large extent. However security is still a major concern for digital and Information and Computer Technology (ICT) society. RF wireless communications suffer from its open nature of RF propagation. This introduces significant challenges in security especially when considering two scenarios: next generation wireless networks with large-scale decentralized features in public areas and point-to-point communications on top-secret issues by very important persons or intelligent agencies as example. While current classical security of wireless network communications relies on classical network cryptography techniques, next generation wireless networks, which possess large-scale decentralized features naturally, will experience high overhead and computational complexity. Several techniques adopted in the standards have been developed in some protocol layers modeled in Open System Interconnection (OSI) layer with less focus given on the physical layer (PHY). Therefore, new technique in physical layer
security has been introduced, in this paper, to be an alternative for such a circumstance. Instead of being based on computational mathematical complexity like others in higher layers such as WEP protocols in Wi-Fi in data (2nd) layer, it enables two wireless entities to communicate data securely in the presence of an eavesdropper through the use of physical layer properties of its inherit channels. There are demands on the development of systems with highly secure, affordable, and efficient features.

The most vulnerable point in wireless communication for intruder attack is the transmission channel. Indeed the interception of OWC signal is far more difficult compared with the RF and the popular techniques available in literature for OWC to overcome intruder are either modulation or encryption based. Modulation schemes based on spread spectrum techniques are commonly used. Spread spectrum performs a data encryption in the modulation process. Wireless Optical Spread Spectrum (WOSS) system is done by using the conventional optical wireless communication devices with some added circuitry which is responsible for applying the spreading technique. Direct Sequence Spread Spectrum (DSSSS) and Time hopping codification in VLC have been presented in [7] and [8] respectively. Optical Code Division Multiple Access (O-CDMA) is the most prevalent technique used in VLC for security as well as for multiple access. O-CDMA have advantages like it provides format independent security in physical layer in addition to the easy-to-implement and de-centralized control network, improved spectrum efficiency and so on [9]. Another conceptual work on optical wireless communication link for telephone networks has been proposed in [10] which deals with the quantum cryptography, quantum teleportation quantum key and quantum coding and decoding can be implemented using OWC link.

Need of secure and reliable communication link is the need of the hour and this paper is addressing these two crucial issues using novel techniques. In order to achieve security, spatial diversity based transmission using two optical transmitters are used and to achieve reliability a new method is proposed for the construction of structured parity check matrix (H) for LDPC codes. Details of these two approaches are discussed in the Section 2 and 4. Some theoretical approaches [11] exists in literature about security but real implementation and demonstration is still not addressed lucidly. Results are presented in 5. Finally conclusion are drawn in Section 6.

2 Proposed scheme

Details of the proposed scheme will be discussed in this section. The purpose of the proposed scheme is to improve the data integrity in physical layer. The concept of the proposed scheme is illustrated by Figure 1.

Two transmitters (I & Q) are used to transmit the information instead of one. The information is split between the two transmitters evenly. If the receiver is in the coverage area of I and Q transmitter, only in that case, it will be able to reconstruct the original information. If the receiver is within the coverage area of one of the two LEDs or

Fig. 1: Position based reception to ensure secure data communication. Only the blue colored receiver can receive successfully. The rest are not successful in terms of reception.
none of the LED, then it will not be able to reconstruct the signal. Thus, it is possible to establish a secure communication link with the desired receiver. For acknowledgement (from receiver to the transmitter), IR is used. For data integrity, a newly proposed method of the construction of $H$ matrix for LDPC codes is used.

### 3 Implementation details

The block diagram of the transmitter (only downlink design) is shown in Figure 2. Uplink design is quite straightforward consisting of IR transmitter and receiver and need not to be explained here.

A quadrature generator is used to generate cosine wave ($I$ signal) and sine wave ($Q$ signal) at a specified frequency. LT1260 is used for this purpose. The schematic diagram for the quadrature generator is shown in Figure 3. By tuning the values of resistors and capacitors, the desired frequency can be achieved.

The output of the quadrature generator will become the input of the multipliers. Multiplier is used with null scaling factor configuration. Random data is generated using a high speed development board. Let us assume that we have a binary data stream which can be expressed as:

$$d_k(t) = d_0, d_1, d_2, d_3$$

where $d_k(t)$ is either +1 or 0. In order to overcome the effect of the channel, channel coding using Low Density Parity Check (LDPC) is implemented and the details will be discussed in the next section. Applying LDPC coding on $d_k(t)$ we get:

$$b_k(t) = d_k(t) + d_{LDPC}(t)$$

where $d_{LDPC}(t)$ are the additional bits which are added in the binary data stream due to the channel coding scheme. Furthermore within the development board, the even and

---

**Fig. 2:** Block diagram of transmitter (downlink design only)

**Fig. 3:** Simulation results of the quadrature generator
odd indexes of $b_i(t)$ is separated which are made accessible through the digital pins. Separated data stream in even and odd indexes can be expressed as:

$$b_i(t) = b_o, b_2, b_4, \ldots \quad \text{(even bits)}$$  \hspace{1cm} (3)

$$b_o(t) = b_1, b_3, b_5, \ldots \quad \text{(odd bits)}$$  \hspace{1cm} (4)

where data rate of $b_i(t) = b_o(t) = b_e(t)/2$. $I$ signal is the product of even indexes of channel coded bits with cosine wave and $Q$ signal is the product of odd indexes of channel coded bits with sine wave. Output of the multiplier is actually the combination of sinusoidal wave and the data which can be expressed as:

$$s_i(t) = \frac{1}{\sqrt{2}} b_i(t) \cos(2\pi f_t t)$$  \hspace{1cm} (5)

$$s_o(t) = \frac{1}{\sqrt{2}} b_o(t) \sin(2\pi f_t t)$$  \hspace{1cm} (6)

The next stage is the amplification and LED driver stage and signal can be expressed as:

$$s_i(t) = A + \frac{1}{\sqrt{2}} b_i(t) \cos(2\pi f_t t)$$

$$= B \times b_i(t) \cos(2\pi f_t t)$$  \hspace{1cm} (7)

$$s_o(t) = A + \frac{1}{\sqrt{2}} b_o(t) \sin(2\pi f_t t)$$

$$= B \times b_o(t) \sin(2\pi f_t t)$$  \hspace{1cm} (8)

where $A$ is the amplification factor. In order to control the current flowing through the LED, a transistor is used in the LED driver stage. Off-the-shelf high bright LEDs (HBLEDs) were used and the built-in control circuit of the HBLED lamp was removed to enhance its switching speed. The transmitted power by the LED can be expressed as:

$$P_t = \int_{\Delta_{\text{min}}}^{\Delta_{\text{max}}} \int_0^{2\pi} \phi \cos(\theta) \, d\phi \, d\lambda$$  \hspace{1cm} (9)

where $\Delta_{\text{max}}$ and $\Delta_{\text{min}}$ should be selected based on photo detector and $\phi$ is energy flux. When the signal goes to the channel, noise will be added by the channel which can be expressed as:

$$s_{\text{CHANNEL},i}(t) = B \times b_i(t) \cos(2\pi f_t t) + n_i(t)$$  \hspace{1cm} (10)

$$s_{\text{CHANNEL},o}(t) = B \times b_o(t) \sin(2\pi f_t t) + n_o(t)$$  \hspace{1cm} (11)

where $n_i(t)$ and $n_o(t)$ are the noise added to each link. The DC channel gain can be expressed as:

$$H(0) = \frac{R(\phi) \cos(\theta) A}{d^2}$$  \hspace{1cm} (12)

where $d$ is the distance between LED and the photo detector, $\theta$ is the angle of incidence, $A$ is the physical area of photo detector. The received power at the photo diode can be mathematically modelled as:

$$P_r = \sum_{\text{LEDs}} \{ P_r H_d(0) + \int_{\text{wall}} P_r d H_{\text{ref}}(0) \}$$  \hspace{1cm} (13)

where $H_d(0)$ is the direct path and $H_{\text{ref}}(0)$ is the reflected path. The received signal can be expressed as:

$$R(t) = B \times [ b_i(t) \cos(2\pi f_t t) + b_o(t) \sin(2\pi f_t t)] + n_r(t)$$  \hspace{1cm} (14)

where $n_r(t) = n_i(t) + n_o(t)$ is the accumulative noise.

Information from both the LEDs will be received from the receiver which consists of photodiode, amplifiers, development board, and a computer (doing post-processing) as shown in the Figure 4. Light falling on the photo diode will generate a current in proportion to the intensity of light. Due to the channel behavior, the signal will be attenuated and weak thus the trans-impedance amplifier (TIA) with a standard well known design is used [12]. The output of TIA will be fed to the differential amplifier for adaptive minimum voltage cancellation. The purpose of minimum voltage canceler is to remove the DC component and the ambient light sources signal from the received signal. Then the signal goes to the development board which records the received information. The last stage is the data processing stage in which MATLAB is used as a tool. The received signal is actually a modulated signal which needs to be demodulated and decoded. For that purpose, the received signal will be first multiplied by the sine wave and then by the cosine wave of the same frequency as used at the transmitter side. As sine and cosine are orthogonal in nature, $I$ and $Q$ signals will be separated. Demodulation can be expressed as:

$$R_i(t) = R(t) \times \cos(2\pi f_t t)$$  \hspace{1cm} (15)

$$R_q(t) = R(t) \times \sin(2\pi f_t t)$$  \hspace{1cm} (16)

After filtering, these separated signals are now combined together with proper indexing to get the binary data. LDPC decoding is also performed at this stage. The received signal is then compared with the transmitted signal in order to calculate the block error rate (BLER).
The block diagram of the receiver is shown in Figure 4. If the receiver is receiving information from both LEDs, the receiver will be able to recover the information correctly. Table 1 gives a quick summary of the components characteristics used in this experimentation and the actual figure for implementation is shown in Figure 5.

### 4 Design of parity check matrix

Channel coding is a hot area of research in order to make the communication link reliable. Today, Low Density Parity Check (LDPC) codes are considered as the most eligible channel codes for future generation high data rate communications and various practical applications. Literature reveals that the random generated parity check matrix performs inferior to structured parity check (\(H\)) matrix. Implementation complexity of LDPC codes can be significantly reduced if an appropriate structured \(H\) matrix is defined [13]. Various researchers have tried to create an efficient \(H\) matrix which can outperform the random generated \(H\) matrix. Progressing Edge Growth (PEG) [14] algorithm is one of the promising algorithms for the generation of suitable \(H\) matrix with high girth. Fan et al. [15] introduced array structured \(H\) matrix that offers comparable performance when compared to random generated \(H\) matrix with low noise floor and no existence of cycle of 4. Eleftheriou et al. [16] proposed a Modified Array Structure (MAC) by applying cyclic shift to Fan’s array which offers superior performance to Fan’s array by reducing number of 1’s in lower triangle. Chutima et al. [17] work is based on MAC in which number of 1’s were reduced...
in upper triangle by applying matrix transpose, and row and column swap which give rise to two new structured $H$ matrix. Singhaudom et al. [18] introduced the Interleaved Modified Array (IMAC) by introducing quasi cyclic matrix into the cyclic shift Fan’s array.

$$\alpha\omega = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \alpha^2\omega^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \alpha^3\omega^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Our work for channel coding is based on the optimization of Chutima’s work by introducing quasi cyclic matrix into the Chutima structured $H$ matrix. By doing so, further reduction in the number of 1’s in $H$ matrix can be obtained leading to a new-sparse $H$ matrix. In order to evaluate the performance of our proposed $H$ matrix, we compared it with PEG, Fan, MAC, IMAC and Chutima $H$ matrix. 6×12 binary $H$ matrix was taken for each algorithm in order to provide a fair comparison. Sum product algorithm was used for LDPC decoding. Generalized form of Fan, MAC, Chutima, IMAC and proposed 6×12 $H$ matrix is shown in Table 2. The generalized form of proposed algorithm is given as follows:

$$H_{PROPOSED} = \begin{bmatrix} I & \alpha\omega & \alpha^2\omega^2 & \alpha^3\omega^3 & \cdots & \alpha^{k-i}\omega^{k-1} & \alpha^k\omega^l \\ 0 & I & \alpha^2\omega & \alpha^3\omega^3 & \cdots & \alpha^{k-i}\omega^{k-1} & 0 \\ 0 & 0 & I & \alpha^2\omega & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & I & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & I & \cdots & 0 \end{bmatrix}$$

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Mathematical Form</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan</td>
<td>$\begin{bmatrix} I &amp; I &amp; I \end{bmatrix}$</td>
<td>Low noise floor and no existence of cycle of 4</td>
</tr>
<tr>
<td>MAC</td>
<td>$\begin{bmatrix} I &amp; \alpha^2 &amp; \alpha^3 \end{bmatrix}$</td>
<td>Cyclic shift to Fan’s array</td>
</tr>
<tr>
<td>Chutima</td>
<td>$\begin{bmatrix} I &amp; \alpha &amp; \alpha^2 \alpha^3 \end{bmatrix}$</td>
<td>Matrix transpose, and row and column swap to MAC for reducing number of 1’s</td>
</tr>
<tr>
<td>IMAC</td>
<td>$\begin{bmatrix} I &amp; \alpha\omega &amp; \alpha^2\omega^2 \end{bmatrix}$</td>
<td>Quasi cyclic matrix to Fan</td>
</tr>
<tr>
<td>Proposed algorithm</td>
<td>$\begin{bmatrix} I &amp; \alpha\omega &amp; \alpha^2\omega^2 &amp; \alpha^3\omega^3 \end{bmatrix}$</td>
<td>Introduced quasi cyclic term in Chutima algorithm</td>
</tr>
</tbody>
</table>

5 Results

As described in the previous section that the LDPC coded binary data will be separated into $I$ and $Q$ channels which will be multiplied by their respective sinusoids. Figure 6 shows the result for this case. This signal is the output of the LED driver which will be fed to the LED for transmission over the channel.

First, we demonstrate that if we transmit single channel and then how we can recover the signal. For example, a square wave is modulated by a sine wave. Figure 7 shows the received signal by the photo diode which will be post-processed to recover the original data.

![Q Channel Transmission Signal](image1.png)

![I Channel Transmission Signal](image2.png)

Fig. 6: Signals fed to LEDs
I and Q channel signals will be received by the photodiode and after amplification will be recorded by the development board and finally fed to the computer for further processing which includes demodulation, filtering, decoding and re-arrangement of bits. Figure 8 shows the received signal at the photodiode after amplification and adaptive minimum voltage cancellation.

Output of photodiode consists of both sine wave and cosine waves. However due to their orthogonal nature we can separate them out using demodulation.

Investigating on the performance of proposed $H$ matrix, results shows that appropriate quasi cyclic shift in $H$ matrix construction have better performance than structured and random generated methods of $H$ matrix construction. Performance of our proposed $H$ matrix is superior to PEG, FAN and MAC $H$ matrix and have comparable performance to IMAC. Comparing the performance with Chutima’s work, the performance of proposed $H$ matrix is superior especially at higher SNR but for low SNR, performance is quite similar. Figure 10 shows the simulation results for Block Error Rate (BLER) against $Eb/No$ under Additive White Gaussian Noise channel.

6 Conclusion

In this paper a novel method for establishing a secure and reliable communication link using optical wireless communication (OWC) is presented. Results show that a secure communication link can be achieved using the proposed approach. Channel degradations can be overcome by implementing suitable channel codes and for this paper, a new method for the construction of parity check matrix for LDPC codes have been presented. Our investigations are limited for static receiver as well as binary LDPC codes. However the proposed method for $H$ matrix generation can also be applied for non-binary LDPC codes for further improvement in BER but at the cost of increased complexity. Our future work will focus on designing the secure communication system for mobile receiver with non-binary LDPC codes for large data length.

Acknowledgments: Mr. Saadi would like to thank for the financial support from 90th Anniversary of Chulalongkorn
University Scholarship. The authors would also like to express gratitude to National Electronics and Computer Technology Center (NECTEC) for partially supporting the research project. Finally, the authors would like to thank Dr. Wasinee Nunpakdee for valuable discussion.

References


