THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

SDR Based PLC and VLC for Indoor Broadband Broadcasting

K. Arun Kumar
Associate Professor, Department of Electronics and Communication
Jeppiaar Institute of Technology, Sriperumbudur, Chennai, Tamil Nadu, India
G. Sathish
Student, Department of Electronics and Communication, Jeppiaar Institute of Technology
Sriperumbudur Chennai, Tamil Nadu, India

Abstract:
In this paper, we propose a novel and cost-effective indoor broadband broadcasting system using power line. Radio Frequency communication technology is overcome by Visible Light Communication (VLC) due to the occurrence of large signal interference. Data is transferred through power by means of Power Line Carrier Communication (PLCC) integrated along with VLC. Software Defined Radio (SDR) is meant for the purpose of securing the data which is transmitted through PLCC modem. Skipjack algorithm uses ASCII code for encryption and decryption.

Keywords: *PLCC, VLC, SDR, Secured data transfer, Indoor broadcasting.*

1. Introduction

With the increasing demands for the indoor broadband multimedia wireless broadcasting services the current radio frequency (RF) based solutions, such as Wi-Fi, digital television terrestrial broadcasting (DTTB), etc have to deal with the serious spectral overcrowding issues, especially in the giant shopping mall or dense residential buildings. In this context, visible light communications (VLC), which utilize the illuminating light-emitting diode (LED) for broadband transmission, offers a huge and unlicensed bandwidth to cope with crowded radio spectrum for highly-localized communication systems. Besides, the VLC technology has many other attractive features, such as worldwide availability, radiation free, high-capacity etc and hence it is considered as an appealing alternative of RF technology for indoor multimedia coverage. The conventional network access solution for VLC is done by connecting the LED lamps to the modem via network cables, which requires less modification of the indoor layout and is cost-effective. The integration of VLC and power line carrier communications (PLCC) comes from the observation that all the LED lamps are connected to the power line and the power line can naturally act as the backbone for VLC while powering the LED lamp. In this way, it will save the additional cables and be easier to be installed. Then orthogonal frequency division multiplexing (OFDM) is applied in the hybrid PLC and VLC system to combat the fading channel and achieve higher spectral efficiency. This project is cost-effective indoor broadband broadcasting system based on the deep integration of PLC and VLC is carried out in the laboratory. A deeply integrated PLC and VLC system is proposed in this project for efficient indoor broadband broadcasting, where the signal in the power line is amplified and forwarded to the LED without decoding and all the LED lamps in one group transmit the same signal. In this way, the broadcasting network could be homogeneous and characterized as a single frequency network (SFN), which avoids complicated network switching for the devices roaming between different LED lamps. The channel of the whole communication link can be modeled as multi-path and thus good performance can be achieved through matured channel estimation and equalization techniques. SDR (Software Defined Radio) which is flexibility and cost effective that allows to modify frequency and modulation such as QPSK, QAM and BPSK. Skipjack algorithm is used for encryption protocol. SDR allows secured data transmission without any data loss or interference.

2. System Model

Fig. 1 generally reviews the system models of the different indoor broadcasting schemes based on PLC and VLC.As shown in Fig. 1(a), in the classical scheme (denoted as
Scheme A), the network cable sends the information to the LED lamps so that they can act as access points (APs) [12], which is quite intuitive. However, this scheme requires large modifications to the indoor cable layout and the specific LED drivers as well as modems must be added to couple the signal from communication cables to the LED, which is complicated and not cost-effective at all. With the development of PLC technologies, researchers start considering the integration of PLC and VLC for indoor signal coverage, since power line can naturally act as the backbone for VLC while powering the LED lamp. In this way, the modifications of the indoor cable layout could be avoided as much as possible, which is more suitable to the existing buildings, particularly, the historic buildings. As illustrated in Fig. 1(b), one possible scheme (denoted as Scheme B) is using the PLC modem to couple the data from the Ethernet to the power line [13]. As shown in Fig. 2, the PLC modem integrated with the decoding and forwarding (DAF) unit is added on each

LED lamp to obtain the needed data from the data bus, i.e., the power line, while the "PLC to VLC" module is equipped to modulate the signal to the light. Hereby, the transmitted signal from different LED lamps could be different according to the request of the devices. Both Schemes A and B directly

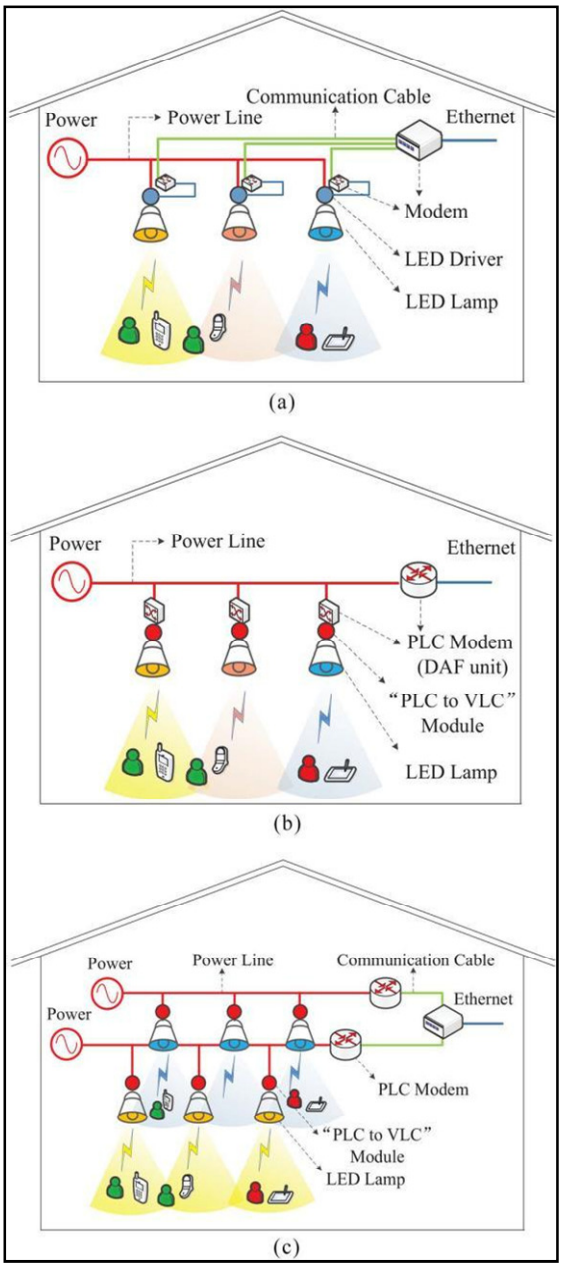

Figure 1: System models of the different indoor broadcasting schemes based on PLC and VLC. (a) Classical VLC-based broadcasting scheme (Scheme A). (b) Classical PLC and VLC-based broadcasting scheme (Scheme B). (c) Proposed deeply integrated PLC and VLC system for indoor broadcasting.

adopt the framework for networking from the idea of the conventional RF based wireless communications, which is quite straightforward but may not well suit for the VLC application scenarios.

Since the visible light signal usually has much less coverage compared to the RF signal, the LED APs should be placed much intensively than the conventional wireless APs

3. Theoretical Analysis

In this section, we will investigate the channel model of the proposed indoor broadcasting system integrated PLC and VLC as well as the noise and interference. In addition, we will also discuss the modulation scheme and SFN for VLC in such scenario. Here "deep integration" or "deeply integrated" means that the modem added to each LED AP is removed and only a "PLC to VLC" module is used so that the baseband signal carried by both PLC and VLC is the same.

3.1. Channel Model

The channel model of our proposed scheme is the cascade of the PLC and VLC parts together with the LED lamp equivalent channel. The channel model of the PLC part can be usually represented by [20]

$$H_{\mathrm{PLC}}(f) = \sum_{l=1}^{L} g_l e^{-(\alpha_0+\alpha_1 f^k)\tau_l v_p} \cdot e^{-j2\pi f \tau_l}$$

(1) where *gl* denotes the weighting factor of the *l*-th path which consists the reflection and transmission factors along this path, $\alpha 0$ and $\alpha 1$

are the attenuation parameters, *k* is the exponent of the attenuation factor (usual values between 0.2 and 1), *vp* is the group velocity and τl is the delay of *l*-th path, and

L represents the number of the paths, respectively. The channel model of the VLC part consists of a line of sight (LOS) component and a diffuse or non-line-of-sight (NLOS) component, which can be written as [9]

$$H_{\mathrm{VLC}}(f) = \eta_{\mathrm{LOS}} e^{-j2\pi f \Delta t_{\mathrm{LOS}}} + \eta_{\mathrm{DIFF}} \frac{e^{-j2\pi f \Delta t_{\mathrm{DIFF}}}}{1 + jf/f_C}$$

(2) where ηLOS, η DIFF, _*t* LOS and _*t* DIFF are the gains and delays

of the LOS and diffuse signals, respectively. *fC* is the 3-dB cutoff frequency of a purely diffuse channel. Hereby, the LOS and NLOS gains are given by [21]

$$\eta_{\mathrm{LOS}} = A_R(r+1)\cos^r\phi \cos\varphi / \left(2\pi d^2\right)$$
$$\eta_{\mathrm{DIFF}} = A_R\rho/(A_{ROOM}(1-\rho))$$

(3), (4)

where *AR* and *AROOM* are the effective receiver area and the room area, respectively.

ρ is the average reflectivity from the

walls. φ and ϕ denote the angles of irradiance and incidence, while *d* is the distance between the LED lamp and the receiver. The Lambert index *r* depends on the half-intensity beam angle $\theta 1/2$, as

$$r = -1/\log_2\theta_{1/2} \quad (5)$$

Moreover, for VLC systems, the white light is usually generated by a device that uses a blue LED for exciting a yellow phosphor coating. Then, the yellow and blue lights jointly create the white illumination. This approach has the advantage of requiring only a single electrically driven source, which is simple and cheap. However, the yellow phosphor has a long decaying time, resulting in that the modulation bandwidth of the LED lamp is constraint to several megahertz. An efficient way to achieve a higher effective bandwidth and higher data rates is to detect only the blue component of the emission with a blue filtering before the receiver, which could expand the bandwidth to dozens of megahertz [10]. In this way, the low-pass impact of the LED lamp could be ignored. Considering the network structure, the channel model for a certain receiver is the superposed effects of all the LED lamps and given by,

$$H(f) = \sum_{i=1}^{N_{\mathrm{LED}}} H_{i,\mathrm{PLC}}(f) H_{i,\mathrm{VLC}}(f)$$

(6)

where *Hi,* PLC *(f)* and *Hi,* VLC *(f)* represent the PLC channel between the PLC modulator and the *i*-th LED lamp, and the VLC channel between the *i*-th LED lamp and the receiver

respectively. *N*LED denotes the number of the LED lamps that the receiver can detect.

3.2. Noise and Interference

A lot of investigations and measurements were achieved in order to give a detailed description of the noise characteristics in a PLC or VLC environment. In the integrated PLC and VLC systems, the noise could be described as a superposition of four noise types listed below, which are distinguished by their sources, time duration, spectrum occupancy, and intensity.

i. Colored background noise [22] is the sum total of various noise sources with low power and varying with frequency. Its power spectral density (PSD) varies over time in terms of minutes or even hours.
ii. Narrowband noise [23], [24] is caused by induction from radio station signals in medium and/or short wave bands. It can be modeled by the sum of several sinusoidal signals and its level is generally varying with daytime.
iii. Impulsive noise [22], [25] is caused by transients due to switching or lightning phenomena within the power network.

The impulses have durations of some microseconds up to a few milliseconds with random occurrence. The PSD of impulsive noise can reach values of more than 50 dB above the background noise. The common statistical model for impulsive noise is the Middleton's Class A model with the parameters of the overlapping factor *A* and the background-to-impulsive noise power ratio _ [23]. Hence, the probability distribution function of the noise amplitude *p(n)* is given by

$$p(n) = \sum_{m=0}^{\infty} e^{-A} \frac{A^m}{m!} \frac{1}{\sqrt{2\pi\sigma_m^2}} e^{-\frac{n^2}{2\sigma_m^2}}$$

$$\sigma_m^2 = \frac{m/A + \Omega}{1 + \Omega} \qquad (8)$$

Moreover, the occurrence of the impulsive noise has approximately a Poisson distribution.

4) Optical background noise [26] arises from sunlight, skylight, incandescent and fluorescent lamps, or other light sources. In practice, the optical background noise could be modeled as additive white Gaussian noise (AWGN).

3.3. Modulation

Since the optical signal is unipolar, any bipolar scheme requires the source to be biased with the aid of a DC offset for the VLC. Consequently, in the previous research, simple modulation schemes such as on-off keying (OOK) and pulse position modulation (PPM) [27] have been extensively adopted for VLC. However, such unipolar modulation schemes suffer from lower spectral efficiency and hence the technique of OFDM with more spectrum-efficient quadrature amplitude modulation (QAM) has been applied in VLC to achieve higher data rates [28].

Considering the fact that OFDM has been widely deployed in the PLC standards and systems to achieve data rates up to gigabits, the OFDM with QAMs are adopted as an appealing modulation solution for the proposed integrated system.

3.4. Single Frequency Network

In our proposed scheme, the transmitters (LEDs) send the same signal on the same frequency band (the light color), which forms a natural SFN [18], [19], [29]. SFN has been widely employed to improve the spectral efficiency and provide reliable as well as robust coverage for DTTB services. Moreover, since the coverage area of each LED lamp is limited, the SFN-like structure could avoid the frequent network switching for the mobile device when roaming under different lamps. The only drawback of SFN structure is that there are severe multipath effects as shown in (6) and thus results in the frequency-selective fading and inter-symbol interference (ISI). Fortunately, this problem could be well solved by the utilization of OFDM, which divides the wideband signal into many narrowband sub-carriers so that each sub-carrier would experience a flat fading channel individually. Furthermore, due to the good spatial directivity of the visible light, such multipath effects will only occur in the overlapping areas.

4. Implementation and Evaluation

4.1. Demonstration Setup

In the laboratorial environment, a demonstration is built and its feasibility is shown through experiments, as shown in Fig.2. The video data is encoded, modulated and coupled to the power line in the PLC modulator. In the "PLC to VLC" module, the signal is added to the DC offset to drive the LED lamp, which is the key component of the integrated system. The signal is detected in the avalanche photo diode (APD), then demodulated and decoded at the receiver. To evaluate the interference of the LED lamps, we use two LED lamps to construct a simplest SFN, as described in Fig. 3. This composition of whole system is quite simple and does not require new installation of communication wiring. After the basic communication modules of the system, such as PLC modulator, "PLC to VLC" module, and the receiver, being plugged in, the system will start to work without too much modification of the existing infrastructures. In fact, such modules can be small enough to be easily installed for commercializing. From implementing the system in real-life,

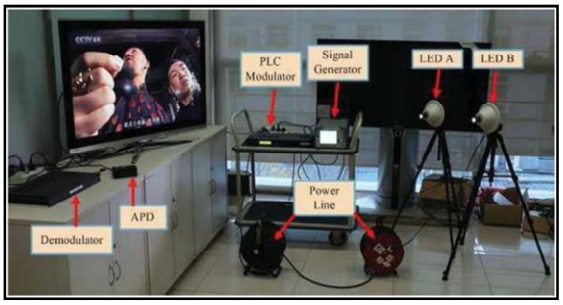

Figure 2: Demonstration setup of the broadcasting system in the laboratorial

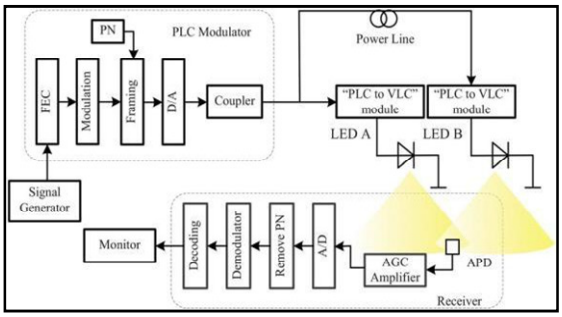

Figure 3: Block diagram of the laboratorial demonstration.

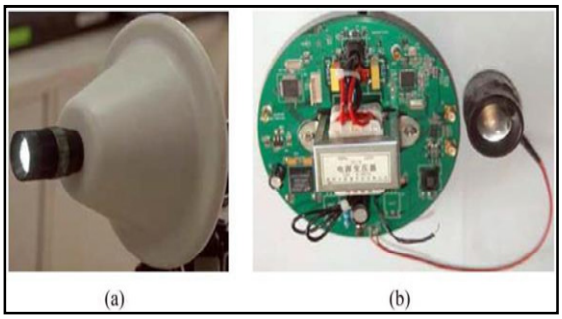

Figure 4: (a) LED lamp. (b) PLC to VLC module.

4.2. Performance Evaluation

The high-definition TV program is modulated by the time domain OFDM (TDS-OFDM), and then transmitted in the hybrid system to evaluate its performance. We use the mode (64QAM, Multi-carrier, PN420, FEC 0.6, TI 720) [30] for the first-step demo.

The system bandwidth is 8 MHz located from 2 MHz to 10 MHz. The point to point system (with one LED lamp on) can still work well with the visible light path up to 8 meters with the interference from the normal indoor lighting devices and provide a date rate of around 48 Mbps within 8MHz bandwidth.

For the two LED lamps, LED A is connected directly to the PLC modulator and LED B is connected to the modulator via a section of power line. Since 3 m is the typical height of the ceilings in many indoor scenarios, the receiver which contains the APD is placed with an equal distance of 3 meters away from the two LED lamps to imitate the case that the receiver is located in the overlapping area or roaming between different LED lamps. In order to evaluate the system performance under different multipath propagations, the length of power line connected to the LED B and the power of the transmitted signal from LED B are set to different values, while the power of the transmitted signal from LED A is fixed in our demonstration configurations.

5. Features of the Proposed System

The integrated system for indoor broadcasting inherits the advantages of both the PLC and VLC systems, and meanwhile overcomes some of their shortcomings, such as the difficulty for mobile coverage in PLC and the “information isolated island” for VLC. The features of the integrated system can be summarized as follows.

5.1. Locatable

The system can be used for indoor positioning due to the excellent directionality of the light and the ubiquity of the LEDs with PLC backbone. Based on the lately VLC techniques, this system can also provide many useful indoor location-based services, including indoor navigation and device tracking [35]–[37]. Moreover, due to the radiation free features, the proposed system is particularly suitable for the indoor hospital applications where the electro-magnetic radiation of the communication systems should be as less as possible.

5.2. High-Capacity

The integrated system inherits the high capacity feature or the ability to support many users simultaneously from VLC system, which is mainly guaranteed by the following three aspects: Broader available bandwidth which is much more than that of the traditional RF band (Wi-Fi or 3G/4G); Wavelength division multiplexing (WDM) which could support different users with different colors of red, green and blue; Space division multiple access (SDMA) which could create parallel spatial pipes by differing spatial locations of the users and hence improve the capacity [38].

Meanwhile, the recent PLC techniques with the data rate up to 1Gbps [39] make it possible to increase the data rate of the whole integrated system to a considerable level. Hence, the proposed system is very suitable for the indoor shopping malls, stadiums, and music halls, where the users are very crowded.

5.3. Easy to Install and Low Cost

For VLC, the integration with PLC is much easier and more natural than with other communication and power supply systems. It can utilize the ubiquitous power line to back up the VLC by adding a small module, which couples the signal from PLC and adds it to the bias current of LED. In this way, the costs on the additional communication lines can be saved and meanwhile the installation can be very easy by adding such module to the LED adapter without any changes to the facilities.

5.4. Data Security

The light waves cannot pass through walls, preventing others from snooping and ensuring the user privacy. Meanwhile, the encryption methods adopted in the traditional communication systems can also be directly applied to the integrated system for enhanced security.

6. Open Issues and Future Work

In this section, we detail some of the promising research areas. These are by no means exhaustive, but outline some important areas where some future work is required.

6.1. MU-MIMO System

In our previous work [8], LED arrays have been utilized to support higher data rates and more reliable signal coverage. In fact, multiple LEDs can be exploited to support multiple users with the aid of multiple input multiple output (MIMO) architectures [6], [40]. This design philosophy is particularly promising, since large arrays of sources/transmitters are relatively straightforward to fabricate and install. Similarly, receiver arrays constituted by hundreds of detectors become feasible in the interest of constructing massive multiple user MIMO (MU-MIMO) systems. By utilizing the lately proposed bit division multiplexing (BDM) [41], the capacity region for the down-link communication of multiple users can be approached. In this way, the system throughput will significantly increase to fulfill the explosive demands for real-time broadband communications.

6.2. Cooperative Optical Communications

Since the predominantly LOS VLC systems exhibit a poor performance in the presence of obstructing objects, it is of great importance to develop cooperative techniques, which are capable of circumventing the problems imposed by LOS propagation. The widespread use of Wi-Fi and mobile broadband services means that future VLC systems will coexist with established RF communications. How best to use these systems cooperatively is still a relatively open research question. The use of VLC hotspots providing very high data-rate connections, combined with RF coverage for reliability, is attractive. In the case of VLC, the ability to visually see the hotspots and move toward them is a further advantage. The analysis disseminated in [42] shows that there is advantage even if only an optical "downlink" is available, which indicates the potential promise of the technique.

6.3. Access Strategy for the Optical Terminals

In the integrated broadcasting network, the optical terminals are usually uncertain about the network state when making decisions. For example, when choosing a VLC hotspot, the optical terminals may not know exactly the reliability and effectiveness of each LED lamp. Besides, the optical terminals have to consider subsequent others decisions to avoid increasing the waiting time and the blocking rate. Recently, the game theory has been introduced into the field to optimize the network protocol and provide the access strategy from the perspective of the users [43]. More research work including the modeling, strategy designing, and so on, is needed to be done.

6.4. Channel Coding for the Integrated PLC and VLC Channel

For indoor VLC and the integrated system, there has been relatively little work on channel coding, since their design has usually followed optical fiber practices, where the information typically remained uncoded [44]. Nonetheless, recently, forward error correction (FEC) coding has been introduced in VLC and the integrated system, combined with OFDM modulation schemes [45]. The channel of the hybrid system is intuitively time-variant due to the volatility of the PLC part and the presence of obstructing objects in the VLC part. Hence, a punctured LDPC and a raptor code adaptively controlled by the transmission rate which accommodates the near-instantaneously fluctuating channel conditions with the aid of a feedback channel need to be investigated.

6.5. Regulations of the Frequency Band

Although VLC offers wider bandwidth compared to the RF solutions, it is still of great necessity to set up some regulations for the segments of the visible light band when integrated with PLC to avoid the communication conflicts and interference, just like the RF band regulations [46]. The regulations should consider the reservation for up-link communications, narrowband services, broadband services, the localization services, the emergency communications for security or alerting notification, and so on. One possible frequency allocation plan is given in Fig. 12, whereby the frequencies below 500 kHz are reserved for the automatic message recording (AMR) based on PLC [47], the frequencies from 500 kHz to 2 MHz are used for narrowband communication, localization, and emergency communication services, while the frequencies above 2 MHz are used for broadband services and up-link communications.

7. Software Defined Radio

Software defined radio technology brings the flexibility, cost efficiency and power to drive communications forward, with wide-

reaching benefits realized by service providers and product developers through to end users. It is any kind of device that wireless transmits or receives signals using visible light communication in the radio frequency (RF) part of the electromagnetic spectrum to facilitate the transfer of information. Traditional hardware based radio devices limit cross-functionality and can only be modified through physical intervention. This results in higher production costs and minimal flexibility in supporting multiple waveform standards. By contrast, software defined radio technology provides an efficient and comparatively inexpensive solution to this problem, allowing multimode, multi-band and/or multi-functional wireless devices that can be enhanced using software upgrades. A number of definitions can be found to describe Software Defined Radio, also known as Software Radio or SDR. The SDR Forum, working in collaboration with the Institute of and Electronic Engineers (IEEE) P1900.1 group, has worked to establish a definition of SDR that provides consistency and a clear overview of the Electrical technology and its associated benefits. Simply put Software Defined Radio is defined as" all of the physical layer functions are software defined

"A VLC device that wirelessly transmits or receives signals in the radio frequency(RF) part of the electromagnetic spectrum to facilitate the transfer of information. In today's world, radios exist in a multitude of items such as cell phones, computers, car door openers, vehicles, and televisions. Traditional hardware based radio devices limit cross-functionality and can only be modified through physical intervention. This results in higher production costs and minimal flexibility in supporting multiple waveform standards. By contrast, software defined radio technology provides an efficient and comparatively inexpensive solution to this problem, allowing multimode, multiband and/or multi-functional wireless devices that can be enhanced using software upgrades.SDR defines a collection of hardware and software technologies where some or all of the radio's operating functions

(also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies. These devices include field programmable gate arrays (FPGA), digital signal processors (DSP), general purpose processors (GPP), programmable System on Chip (SOC) or other application specific programmable processors. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware.

7.1. Software Analysis

The main purpose of using the microcontroller in our project is because high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. By combining a versatile 8-bit CPU with in-system programmable Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcontroller which provides a highly-flexible and cost-effective solution to many embedded control applications. The programs of the microcontroller have been written in Embedded C language and were compiled using KEIL, a compiler used for microcontroller programming. The communication between PC and the microcontroller was established MAX 232 standard and those programs were also done in C language.

7.2. Keil Compiler

The C programming language is a general-purpose, programming language that provides code efficiency, elements of structured programming, and a rich set of operators. C is not a big language and is not designed for any one particular area of application. Its generality combined with its absence of restrictions, makes C a convenient and effective programming solution for a wide variety of software tasks. Many applications can be solved more easily and efficiently with C than with other more specialized languages. The Cx51 Optimizing C Compiler is a complete implementation of the American National Standards Institute (ANSI) standard for the C language. Cx51 is not a universal C compiler adapted for the 8051 target. It is a ground-up implementation dedicated to generating extremely fast and compact code for the 8051 microprocessor. Cx51 provides you the flexibility of programming in C and the code efficiency and speed of assembly language. Since Cx51 is a cross compiler, some aspects of the C programming language and standard libraries are altered or enhanced to address the peculiarities of an embedded target processor.

7.3. Skipjack Algorithm

Skipjack is a 64-bit block cipher that is used in the Clipper Chip. The design principles of Skipjack and the algorithm itself was only recently made public by the NSA. Skipjack is a remarkably simple cipher, and one interesting feature is the use of two different types of rounds. These are referred to as A, and B-rounds and encryption with Skipjack consists of applying 8 A-rounds, then 8 B-rounds, once again 8 A-rounds and 8 B-rounds. Earlier papers have demonstrated that the number of rounds was apparently not chosen with a large margin of security, but they did not focus on the high-level structure of Skipjack. The structure of Skipjack, focusing especially on understanding the rationale behind the design choices embodied in the cipher. A central motivation is the observation that Skipjack is just one representative from a very large design space of related ciphers, and in particular there are many parameters which could easily be changed to get a different construction with presumably different properties. Consequently, it is natural to wonder whether the designers of Skipjack missed any opportunities to improve the cipher by selecting design

This document provides details of the SKIPJACK algorithms. The algorithms are supported in single chip crypto processor such as CLIPPER (SKIPJACK). SKIPJACK uses codebook encrypt /decrypt algorithm.

3.1 Skipjack modes of operation

SKIPJACK is a 64-bit codebook utilizing an 80-bit crypto variable. The modes of operation are a subset of the FIPS-81 description of modes of operation for DES [1]. These include:

Output feedback mode 64bit

Cipher feedback mode 64bit/32bit/16bit/8bit

Codebook 64bit
Cipher-block chaining 64bit

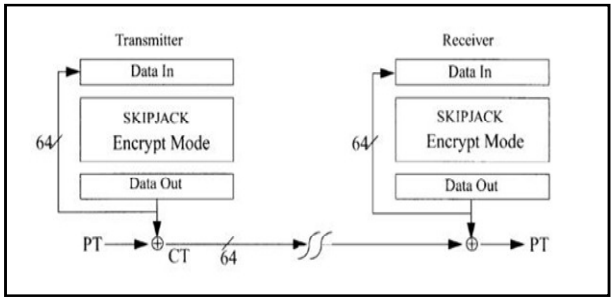

Figure 5: Output feedback mode

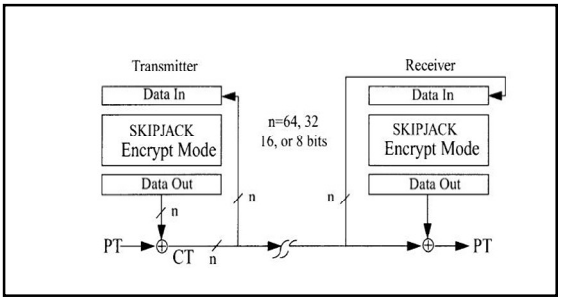

Figure 6: Cipher feedback mode

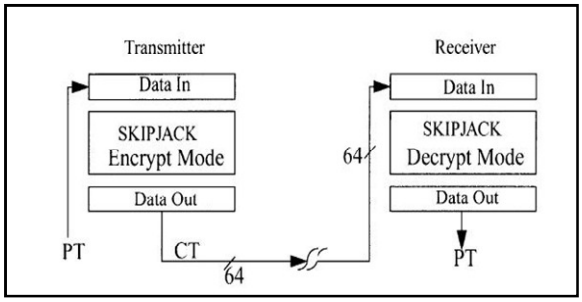

Figure 7: Codebook mode

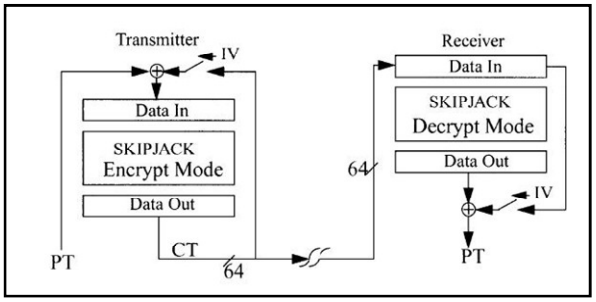

Figure 8: Cipher block chaining mode

3.2 Skipjack specification

1. Notation and terminology

V: the set of all n-bit values. Word: 16-bit value
Byte: 8-bit value

Permutation on v: an invertible (one to one and onto) function from Vn to Vn. That is, the value is permuted within Vn, not the bits within the value.

2. Basic structure:

Skipjack encrypts 4-word (i.e.,8-byte) data blocks by alternating between the two stepping rules (A and B) shown below. A step of rule A does the following

a. G permutes W1,
b. The new W1 is the XOR of the G output, the counter, and W4,
c. Words W2 and W3 shift one register to the right
d. The new W2 is the G output
e. The counter is incremented by one.

Rule B works similarly

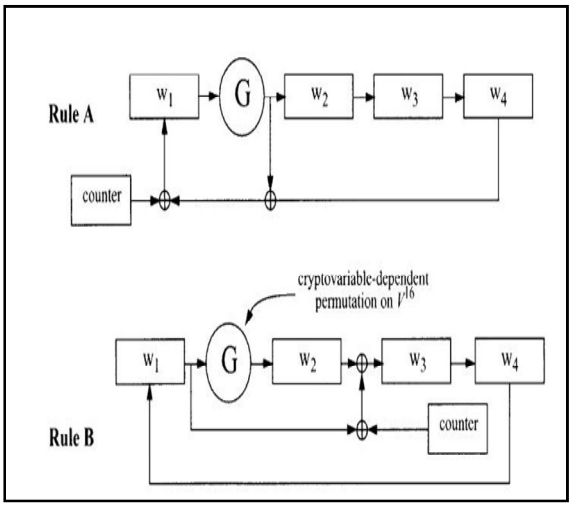

Figure 9: Skip jack stepping rules

3. Stepping rule equations: In the equations below, the superscript is the step number.

ENCRYPT

Rule A	Rule B
$w_1^{k+1} = G^k(w_1^k) \oplus w_4^k \oplus counter^k$	$w_1^{k+1} = w_4^k$
$w_2^{k+1} = G^k(w_1^k)$	$w_2^{k+1} = G^k(w_1^k)$
$w_3^{k+1} = w_2^k$	$w_3^{k+1} = w_1^k \oplus w_2^k \oplus counter^k$
$w_4^{k+1} = w_3^k$	$w_4^{k+1} = w_3^k$

DECRYPT

Rule A^{-1}	Rule B^{-1}
$w_1^{k-1} = [G^{k-1}]^{-1}(w_2^k)$	$w_1^{k-1} = [G^{k-1}]^{-1}(w_2^k)$
$w_2^{k-1} = w_3^k$	$w_2^{k-1} = [G^{k-1}]^{-1}(w_2^k) \oplus w_3^k \oplus counter^{k-1}$
$w_3^{k-1} = w_4^k$	$w_3^{k-1} = w_4^k$
$w_4^{k-1} = w_1^k \oplus w_2^k \oplus counter^{k-1}$	$w_4^{k-1} = w_1^k$

4. Stepping sequence: The algorithm requires a total of 32 steps.

a. To encrypt: Start the counter at 1. Step according to Rule A for 8 steps, then switch to Rule B and step 8 more times. Return to rule A for the next 8 steps then complete the encryption with 8 steps in ruleB. The counter increments by one after each steps.

b. To decrypt: Start the counter at 32 step according to Rule B inverse for 8 steps then switch to rule A inverse for 8 more times. Return to rule B inverse for next 8 steps then complete the decryption with 8 steps in rule A inverse. The counter decrement by one after every step.

5. G-permutation:

The crypto variable depended permutation G on V16 is a four round feistel structure. The round function is fixed byte substitution table which will be called F table. Each round of G also incorporates a byte of crypto variable. This Give two characterization of the function below

A. Recursively:

$$g_3 = F(g_2 \oplus cv_{4k}) \oplus g_1$$
$$g_4 = F(g_3 \oplus cv_{4k+1}) \oplus g_2$$
$$g_5 = F(g_4 \oplus cv_{4k+2}) \oplus g_3$$
$$g_6 = F(g_5 \oplus cv_{4k+3}) \oplus g_4$$

Similarly, for the inverse, $[G^k]^{-1}(w = g_5 \| g_6) = g_1 \| g_2$ where

$$g_{i-2} = F(g_{i-1} \oplus cv_{4k+i-3}) \oplus g_i .$$

Schematically

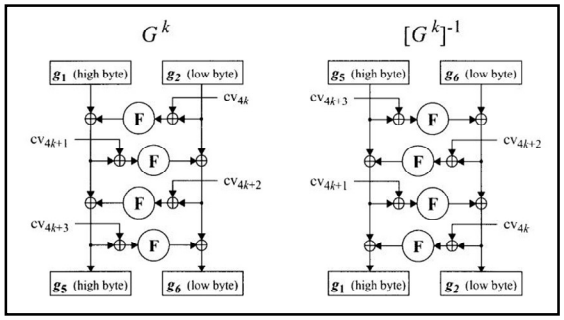

Figure 10: G- Permutation

6. Crypto variable schedule:

Crypto variable is 10 bytes long and used in its natural order so the schedule subscript given in the definition of the G permutation are to be interpreted mod10

7. F-table:

The skipjack F-table is given below in hexadecimal notation. The high order 4-bit of the input index row and the lower order of the 4-bit in the indexed column. For example, F(7a) = d6

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	a3	d7	09	83	f8	48	f6	f4	b3	21	15	78	99	b1	af	f9
1x	e7	2d	4d	8a	ce	4c	ca	2e	52	95	d9	1e	4e	38	44	28
2x	0a	df	02	a0	17	f1	60	68	12	b7	7a	c3	e9	fa	3d	53
3x	96	84	6b	ba	f2	63	9a	19	7c	ae	e5	f5	f7	16	6a	a2
4x	39	b6	7b	0f	c1	93	81	1b	ee	b4	1a	ea	d0	91	2f	b8
5x	55	b9	da	85	3f	41	bf	e0	5a	58	80	5f	66	0b	d8	90
6x	35	d5	c0	a7	33	06	65	69	45	00	94	56	6d	98	9b	76
7x	97	fc	b2	c2	b0	fe	db	20	e1	eb	d6	e4	dd	47	4a	1d
8x	42	ed	9e	6e	49	3c	cd	43	27	d2	07	d4	de	c7	67	18
9x	89	cb	30	1f	8d	c6	8f	aa	c8	74	dc	c9	5d	5c	31	a4
Ax	70	88	61	2c	9f	0d	2b	87	50	82	54	64	26	7d	03	40
Bx	34	4b	1c	73	d1	c4	fd	3b	cc	fb	7f	ab	e6	3e	5b	a5
Cx	ad	04	23	9c	14	51	22	f0	29	79	71	7e	ff	8c	0e	e2
Dx	0c	ef	bc	72	75	6f	37	a1	ec	d3	8e	62	8b	86	10	e8
Ex	08	77	11	be	92	4f	24	c5	32	36	9d	cf	f3	a6	bb	ac
Fx	5e	6c	a9	13	57	25	b5	e3	bd	a8	3a	01	05	59	2a	46

Figure 11: Skipjack matrix

8. Conclusion

Our next step for the demonstration is to try higher order constellation mapping and wider band occupation to fully utilize the system potential. We have implemented the off-line VLC system with a data rate of 481Mbps in a 100 MHz bandwidth [7] and are working on the real-time integrated system with a date rate of 192 Mbps in a 24 MHz bandwidth. At the same time, some efficient techniques, such as the Gray amplitude phase shift keying (APSK) constellation [48], the appropriate channel coding, MIMO and the relays [13], [49], [50], will be adopted as the system options to enhance the robustness and throughputs of the system and satisfy different quality of services. Moreover, we will investigate the handover or switching protocols discussed in Section II. The prototypes integrated with the simplified network and access protocol will be implemented as well. Meanwhile, as shown in Fig. 12, we have implemented a laboratory demo with an Android APP for indoor localization and communication based on VLC and also started the implementation of a lower data rate (up to several kbps) communication system by utilizing the commercial camera of the mobile phones with the interface permissions from the mobile phone manufacturers. Considering the needs that the integrated system can still work during day-time, some techniques to ensure the communication performance under illuminance constraints and various dimming constraints should be investigated. Such work could speed the commercialization of our proposed systems and prototypes.

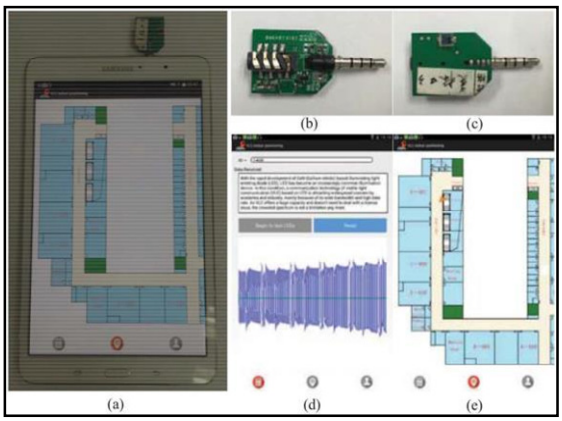

Figure 12: Demo and Android APP for indoor localization based on VLC.

(a) Demo. (b) Receiver (back). (c) Receiver (front). (d) Signal detection in the Android APP. (e) Map localization in the Android APP.

This method helps us in efficient data transmission using power line and visible light communication with software defined radio which has been constructed using visual basic. The proposed system improves accuracy, speed and security for data in real life scenario and is suitable for transmission. This is extremely useful in places where very high values data are transferred and can be extensively used in offices. We also suggest that the use of use of power line and visible light may improve the efficiency to a higher level.

9. References

i. J. Rufo, J. Rabadan, F. Delgado, C. Quintana, and R. Perez-Jimenez (2010), "Experimental evaluation of video transmission through LED illumination devices," Vol 56,pp 1411–1416.
ii. Abhishek Singh, Prof. Anil Mishra (2015),"Checking the feasibility of power line communication channel with noise using OFDM Technique" , Vol 2, pp1094 – 1102.
iii. O'Brien1a Hoa Le Minha, Lubin Zenga and Grahame Faulknera (2008),"Indoor Visible Light Communications: challenges and prospects", Vol7 pp1-9.
iv. Anurag sarkar and Prof. Shalabh Agarwal(2015)," LI-fi Technology: Data Transmission through visible light", Vol 3, pp1-12.
v. Hao Dong, Hongming Zhang and Kai Lang (2014), "OFDM visible light communication transmitter based on LED array", Vol 3 pp1-4.
vi. Gianmarco Baldini and Taj Sturman (2012), "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A survey and a way ahead",Vol 14 pp 355-379.
vii. Y.Ganjdanesh and M.Moosavi(2003) , "Voltage control oscillator design for software-define radio in wideband", Vol 3 pp 12-16.
viii. Lars Knudsena and David Wagnerb (2000), "On the structure of Skipjack algorithm", Vol 2 pp13-16.
ix. Yingjie He, Liwei Ding, Yuxian Gong, and Yongjin Wang (2013), "Real-time Audio & Video Transmission System Based on Visible Light Communication",vol 3 pp153-157.
x. RajanSagotra and Aggarwal(2013), " visible light communication", vol 4 pp403-405.
xi. Santiago Arag and Federico Kuhlmann(2015), "SDR-based network impersonation attack in GSM-compatible networks",vol3 pp 1-6.
xii. Rafael Montalban, Jos´e, A. L´opez-Salcedo and Gonzalo(2013)," Power Allocation Approaches for Combined Positioning and Communications OFDM Systems",Vol 3 pp26-32.
xiii. Stefan Schmid and Giorgio Corbellini(2012), "An LED-to-LED Visible Light Communication System with Software-Based Synchronization", vol 2 pp 1-5.
xiv. Chi-Yuan Chen1and Fan-Hsun Tseng(2010), Reconfigurable Software Defined Radio and Its Applications, Vol13 pp 29-37.
xv. Abdul Manna and D. K. Saxena (2014), "A Study on Power Line Communication", vol 4 pp 1-4.
xvi. Baihua Shen and, Guoli Wang(2013), "Distributed target localization and tracking with wireless pyroelectric sensor networks", vol 6 pp 1400- 1418.
xvii. K.VasudevanandSivaraman (2010),"Software DefinedRadio Implementation(With simulation & analysis)",vol 4 pp21-27.
xviii. Ms.Neha,R. Laddha, A. P. Thakare (2013), "A Review on Serial Communication by UART", vol 3pp 366-369.
xix. Sameer and Dinesh Mohadikar (2016) ,"Digital Integrated Circuit Tester Using AT89S52",vol6 pp263-267.
xx. Muhammad Islam, M A Hannan, S. A. Samad and A. Hussain (2009), " Software Defined Radio for RFID Application", vol 1 pp1-4