5-24-2018

Stealth transmission in free space optical communication systems using amplified spontaneous emission noise

Youness Ergaibi
Rowan University

STEALTH TRANSMISSION IN FREE SPACE OPTICAL COMMUNICATION SYSTEMS USING AMPLIFIED SPONTANEOUS EMISSION NOISE

by

Youness Ergaibi

A Thesis

Submitted to the
Department of Electrical & Computer Engineering
College of Engineering
In partial fulfillment of the requirement
For the degree of
Master of Science in Electrical & Computer Engineering
at
Rowan University
May 2, 2018

Thesis Chair: Ben Wu, Ph.D.

Dedication

I would like to dedicate this work to my parents for all their love, support, and sacrifices. Without them, I would not have been able to get to this stage of my life. I also want to express my sincere gratitude to my brother Abdelhakim, my family, and my friends.

Acknowledgements

I would like to thank my advisor, Professor Ben Wu, whose motivation, enthusiasm and hard work have greatly inspired me. I am grateful to him for his encouragement and constant guidance throughout this journey, making this work possible. I also would like to extend my gratitude to Dr. Nidhal Bouaynaya and Dr. Nasrine Bendjilali for being a part of my committee and for their generous time and commitment. Special thanks to Yang Qi, who has been very helpful and a team player in this work. Finally, I would like to thank other fellow researchers and teaching fellow students that I had the opportunity to meet and work with.

Abstract

Youness Ergaibi
STEALTH TRANSMISSION IN FREE SPACE OPTICAL COMMUNICATION SYSTEMS USING AMPLIFIED SPONTANEOUS EMISSION NOISE
2017-2018
Ben Wu, Ph.D.
Master of Science in Electrical & Computer Engineering

One of the challenging real-world problems in the communication network is to secure the communication system that deals with a large data. Perhaps even a more challenging version of this scenario is when the channel that transmits the information is a wireless media. This thesis introduces a steganography technique to secure the physical layer of the communication system. It enhances the benefits by using optical communication rather than radio frequency (RF) communication, especially in terms of transmitting a large scale of data. This thesis demonstrates that we can transmit secure large information in free space (air) using steganography mechanism and free space optical (FSO) channel. In this work, we built a secure optical wireless communication prototype. We analyzed the performance of this system using eye diagram and bit-error rate (BER) measurements. The application of this work can be used in many applications such as monitoring enterprise and campus connectivity, smart sensors and internet of things networks.

Table of Contents

Table of Contents (Continued)

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation: Building a Secure Communication Network System With a High Speed Which Considers its Application on Cyber-Physical Systems (CPSs)

Nowadays, we have been noticing an immense deployment of smart grid systems, autonomous automobile systems, medical monitoring, process control systems, and robotics systems in large scale. The common point of those systems is the control or monitoring that is done by computer-based algorithms, tightly integrated with the Internet and its users, which means that there is a high possibility to be attacked and damaged. Those systems are called cyber-physical systems (CPSs).

This increasing deployment of those types of technology, requires and involves taking care of security and high speed in micro and macro levels [1, 2]. Most of the sensors and nodes of CPS communicate using the wireless networks, and it is well known that the spectra of radio frequency are well occupied by other protocols and standards (Wi-Fi, AM/FM audio radio wave, LTE, 4G), which involves optimizing the RF spectrum or switching on another type of communication channels in order to ensure data capacity and security of the CPS systems. Those requirements become more challenging when we know that the more we try to secure a communication channel, the more we need a large data capacity. For instance, one technique to secure data privacy is to use cryptography, and it is well known that the bigger key length is, the more the system is secure. Therefore, any secure system of communication requires the consummation of the high amount of data capacity.

1.2 Problem Statement

The cyber physical systems are in accelerating development because of the high demand for those systems, which leads to create a large amount of the CPS access points and nods to satisfy the deployment. As a result, that requires using an extraordinary load of the RF spectrum (which is already well occupied) with dealing with sensitive and private information. Therefore, all those reasons drive the designer to look for a balance between security and data capacity in those systems.

The RF spectrum is between 300 KHz and 30 GHz. The question is how to use efficiently this band, or increase this spectrum especially for the CPS application, at the same time ensure the security of wireless communication systems. There are two approaches that deal with this challenge. One scenario is to use the RF spectrum efficiently via the technique of the cognitive radio [3–7]. Basically, this method involves using specific RF bands so that when any band is idle, it can be allocated directly. The other scenario is to remove all types of interference, especially the self-interference and the overlapping spectra. This scenario involves using the orthogonal frequency division multiplexing (Self-interference) [8–12], and blind source separation (overlapping spectra) [13–17]. All of these approaches target the increasing and use the RF spectrum efficiently.

Even those scenarios optimize the RF bandwidth, they still are limited because the RF spectrum is not enough for cyber physical systems that consume a huge amount of data, and more when we add the layer of security. All these approaches increase the spectrum in a smart way. While the limit of all these approaches is the fundamental physical law of electromagnetics, there is only one set of RF spectrum to use.

1.3 Scope of Thesis

The goal of this thesis is to build a communication system that takes into account a balance between security and the need of high data capacity to deal with Cyber-Physical Systems such as smart sensors networks. The idea of using RF spectrums or to even enhance the radio frequencies efficiently (radio cognitive, blind source technique) is dismissed because of the high demand of data capacity in cyber physical systems and the insufficient capacity in the traditional bandwidth of RF spectrum. The possibility of using 5^{th} generation mobile presents a solution in terms of the capacity because the carrier frequency of those networks goes up 70 GHz. However, in this proposed system, we propose using a huge spectrum outside of the traditional RF spectrum, which is between 300 KHz and 30 GHz. The optical spectrum is between 192 THz and 750 THz, which represents at least 10,000 times larger than the bandwidth of the RF spectrum. In this thesis, we will use the optical spectrum to transmit the information in a high data rate. For security, we use analog steganography mechanism to hide the private data (stealth channel) using an amplifier source wideband noise that prevents data from being detected by the eavesdropper. To make this communication system more adaptable to Cyber-Physical Systems (CPS), we use a free space optical (FSO) transmitted channel that hides the stealth channel underneath the public channel which is a wideband source noise generated by the ASE.

1.4 Research Contributions

The primary focus of this thesis, as mentioned above, is to build a secure communication system that balances the security and data capacity using the FSO channel in order to be adaptable to CPS application such as communication between smart sensors. After

building this prototype of system communication using analog steganography to secure the communication, ensuring the data capacity by using the range of optical frequencies between 192THz-197THz, and making it more adaptable to cyber physical systems such as smart sensor networks [18] by using a free space optical link, we analyze the performance of our system using eye diagram and the measurement of Bit Error Rate (BER) measurement. The core contributions and findings of this work are as follows:

1. Demonstration of analog steganography that allows hiding the stealth signal underneath public channel (Security).

2. Ensuring a high speed in a communication system by using optical light wave frequencies that carry the private data. (Data capacity).

3. Implementation of the free space optical (FSO) channel to transmit the data in order to use this channel for cyber-physical systems (CPSs) applications.

1.5 Organization of the Thesis

Chapter 2 provides an overview and background for optical communication systems, the free space optical (FSO) systems, and the security in the physical layer of those systems. A stealth optical communication system that uses an amplified spontaneous emission (ASE) noise is in free space. The results and analysis of the experiment are given in the Chapter 3. Finally, the conclusions and the suggestions for future work are discussed in Chapter 4.

Chapter 2

Background

This chapter provides a comprehensive background review and technical details of optical communication systems that transmit high data capacity, different mechanisms to secure the physical layer of those systems, and finally, the free space optical communication systems.

2.1 Optical Communication System

A communication system transmits data or information from one place to another. It can be a distance of kilometers or a higher distance such as transoceanic distance. An electromagnetic wave carries this information. According to the frequency of this electromagnetic wave, we can determine the type of the communication system. There are different frequencies in the electromagnetic spectrum. The Figure 1 shows various types of the electromagnetic radiations (radio, microwave, infrared etc.), and their ranges in term of frequencies and wavelengths. Any information or data can be carried by those electromagnetic waves, which varies from megahertz to one hundred terahertz. In physics, the wavelengths and frequencies are related according to this equation: $\lambda = \frac{c}{f}$ where λ is the wavelength, f is the frequency and c is the speed of light (c$\approx 3 \times 10^8$ m/s).

There are various types of communication systems: RF communications systems or wireless communication systems that use a radio spectrum and optical communication systems or lightwave communication systems. In general, the bandwidth of RF systems is between 300 KHz and 30 GHz. Lightwave systems use high carrier frequencies in the visible or near infrared division of the electromagnetic spectrum (~ 100 THz). One of

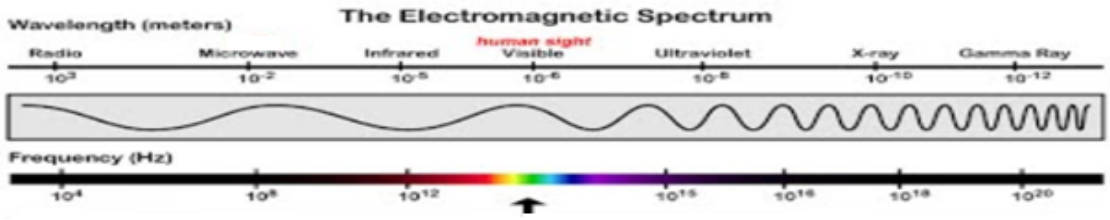

Figure 1. The electromagnetic spectrum

Table 1

Different categories of the communication systems with their ranges of frequencies and wavelengths

Category	Range of Wavelengths (nm)	Range of Frequencies (Hz)
Gamma rays	< 1	$> 3 \times 10^{17}$
X-rays	1-10	3×10^{16} - 3×10^{17}
Ultraviolet light	10-400	7.5×10^{14} - 3×10^{16}
Visible light	400-700	4.3×10^{14}-7.5×10^{14}
Infrared	700-10^5	3×10^{12}- 4.3×10^{14}
Microwave	10^5-10^8	3×10^{9}- 3×10^{12}
Radio waves	$> 10^8$	$< 3 \times 10^9$

those systems is fiber-optic communication system. Table 1 represents a list of different categories of the communication systems with their ranges of frequencies and wavelengths.

The metric that is often used to measure the performance of communication systems is called bit rate-distance product, BL, where B is the bit rate and L is the repeater spacing or the length of transmission link. As the technology has advanced over the years, we have discovered high communication systems with a BL very high. Figure 2 shows the values of bit rate-distance of different types of communication systems. Optical or lightwave communication systems offer a high data rate of transmission comparing to RF

communication systems.

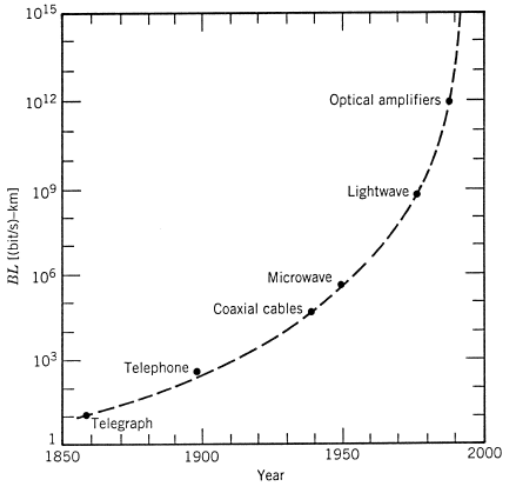

Figure 2. The values of bit rate-distance product of different types of communication systems [19]

2.1.1 Components of the optical communication systems. There are three mains elements of any optical communication systems: optical transmitter, communication channel, and the optical receiver (Figure 3).

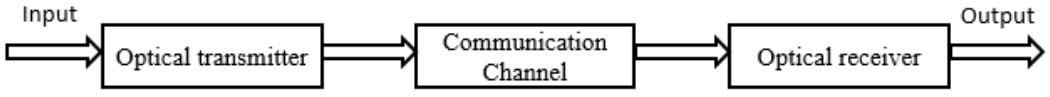

Figure 3. Generic optical communication system

There are two types of the optical communication systems: guided and unguided lightwave systems. The guided systems use directed communication channel, which means

the light transmitted in a way remaining confined spatially (Fiber optic communication systems). Unguided systems, however, use an undirected communication channel, which means the beam transmitted through a broadcasting method in the air (free optical communication systems).

2.1.1.1 ***Optical transmitter.*** The main goal of the transmitter is to convert the electrical signal into an optical signal in order to send this signal into the communication channel such as a fiber optics. The transmitter is composed of three key elements: optical source, modulator, and channel coupler (Figure 4).

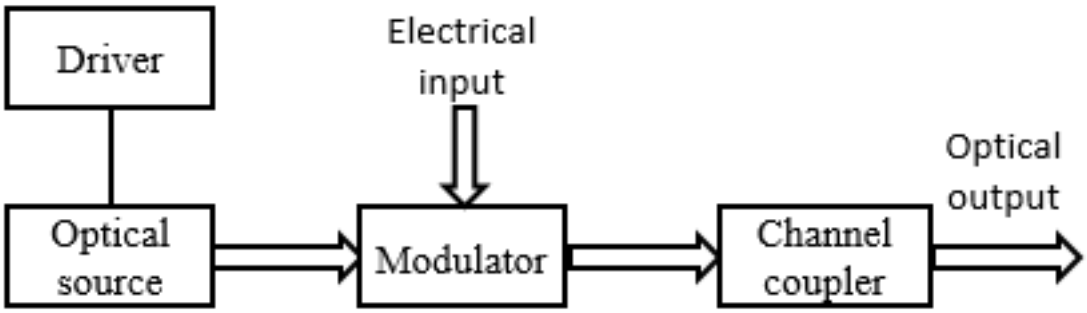

Figure 4. Components of an optical transmitter

Semiconductor laser and light emitting diode are the examples of the optical source. For the modulator, the concept of modulation is to transfer the data to be transmitted from the electrical to the optical domain. There are two approaches to perform the modulation: direct and external modulation. Direct modulation: In this type of the process, the output light of the optical source depends directly on the input drive current. The light is transmitted to the channel coupler when the driver current sends the binary “1” and the light is

blocked when “0” has sent it from the driver. In other words, we vary the injection current of the optical source. External Modulation: In this type of modulation, we include an external device that changes and modulates the intensity or phase of the light signal source. The light source is continuous and kept on, and the external device acts as a switch which is controlled by the information that we want to transmit. The third element of the transmitter is the coupler. The role of this device is to focus on the optical signal received after modulation onto the entrance plan of the communication channel in order to have the maximum of efficiency. This coupler is composed of the microlens.

2.1.1.2 ***The optical communication channel.*** The optical communication channel is one important element of the communication system. The mission of this component is to transmit the optical signal from the transmitter to the receiver. This channel can be free space (transmission in the air Figure 5) or it can be a fiber optic. Most of the lightwave systems used fiber optics as the communication channel due to the silica technology of the fiber optics that transmit the beams light with the losses less than 0.2 dB/km. Historically, during the early 1970s, the loss of the fiber is higher. It was about 20 dB/km. With the advanced technology in photonics, the modern fiber can reach a fiber loss of the 0.2 dB/km. As a mentioned above, the communication channel can be a free-space optical channel. It means that we transmit the data wirelessly by using the light propagating in the free space (air, atmosphere).

2.1.1.3 ***Optical receivers.*** The goal of the optical receiver is to convert the optical signal that is received from the end of the channel communication into the original electrical signal. It is composed of three key elements: coupler, a photodetector, and a demodulator (Figure 6).

Figure 5. Free space channels [20]

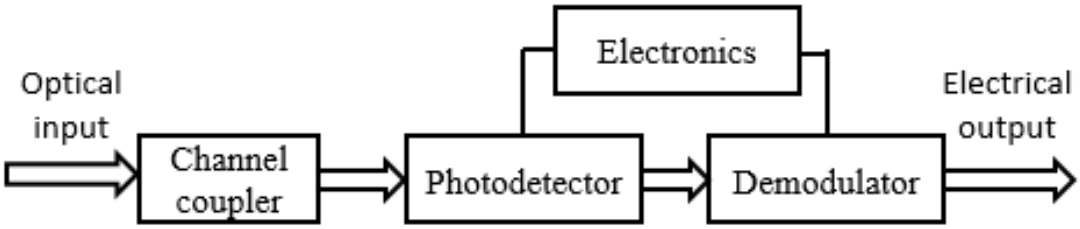

Figure 6. Components of an optical receiver

The coupler focuses the received optical signal onto the photo detector. The components of the photodetectors are, most of the time, the semiconductor photodiodes. The demodulator plays the role of recovering the data that has been transmitted in a modulation technique. The demodulator that is used in the optical receiver depends on the format of modulation that is already used. For example, if we use the frequency shift keying (FSK) or phase shift keying (PSK) in the modulation, we should use the heterodyne or homodyne detection for demodulation. Most of the lightwave systems use a scheme referred to intensity modulation with direct detection (IM/DD). In this case, the demodulation is done by a

decision circuit that identifies bits as “1” or “0,” depending on the amplitude of the electrical signal. One technique of demodulation is called homodyne detection. It is a process of extracting information from a message that modulated in-phase or in-frequency of an oscillating signal. This technique is based on comparing a signal with a standard oscillation that would be identical if it carried null information. To recover the information using the homodyne detection, the signal interferes with itself. It is easy to see the phenomena of homodyne detection by using a Mach-Zehnder (MZ) interferometer structure [21].

2.1.2 The performance of the optical communication systems. There are many ways to measure the performance of the optical communication systems. In this section, we propose three methods: Eye diagram, bit-error rate (BER) and the signal to noise ratio (SNR).

2.1.2.1 ***Eye diagram.*** It is also called an eye diagram. It is a display of an oscilloscope. The digital signal (bits “1” and “0”) from the receiver is repetitively sampled. Those “0” and “1” bits are applied to the vertical input. However, the horizontal sweep is triggered by the data rate of the signal. The pattern in output looks like a series of eyes. The eye diagram is a good tool to see and evaluate the effect of the channel noise and intersymbol interference on the performance of a pulse transmission system. This is how it looks like an eye diagram (Figure 7). By analyzing the eye diagram, we measure the performance of the system. An open and clear eye pattern corresponds to minimal signal distortion and noise signals in the system.

2.1.2.2 ***Bit-error rate (BER).*** It is a criterion that measures the performance of the optical communication system by measuring the receiver sensitivity of the system. A

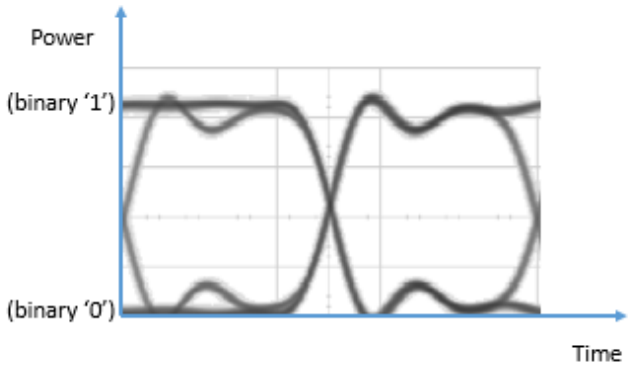

Figure 7. Eye diagram

receiver is said to be more sensitive in case it reaches the same performance with less optical power incident. The BER is the probability of the incorrect identification bit by the decision circuit of the receiver. Therefore, a BER of 2 $\times 10^{-9}$ corresponds to on average of 2 errors per 10^9 bits. For the digital optical receivers, they require the BER to be below 10^{-9}.

2.1.2.3 ***Signal to noise ratio (SNR).*** Signal to noise ratio (SNR) is a parameter that defines and compares the level of the desired signal to the background's level of the noise. It is the ratio of signal power to the noise power. It is often expressed in decibels (dB). An SNR greater than 0 dB means that we have more signal than noise. In the optical communication systems, the signal to noise ratio (SNR) is defined as follows:

$$SNR = \frac{average\,signal\,power}{noise\,power} = \frac{I_p^2}{\sigma^2} = \frac{I_p^2}{\sigma_T^2 + \sigma_s^2} \tag{2.1}$$

Where I_p is the photocurrent and σ^2 is total noise at the receiver including shot noise σ_s and thermal noise σ_T.

2.1.3 Summary. In this section, we talked about different categories of the communication systems including RF communication and optical communication system. We also depicted the components of the optical communication system. The idea behind this section is to show the opportunity that optical communication systems offer comparing to the RF communication. Those systems allow a high data rate of transmission because of the huge bandwidth of the optical spectrum. The bandwidth of the RF is limited and it is no longer a valid choice for new applications that require a high data capacity. We concluded by proposing methods to calculate and analyze the performance of those systems.

2.2 Security in the Physical Layer of the Optical Communication Systems

2.2.1 Introduction. In computer networking, the world is experiencing an exponential growth of using fiber optics networks comparing to the cable coaxial networks. This is due especially to the high capacity and bandwidth of the fiber optics. That is why we actually see that the backbone of the internet is occupied by the fiber optics networks. The physical layer in open systems interconnection (OSI) model [22] is integrally constituting of fiber optics. There is a correlation between the physical layer and six layers above in term of security. Implementing security (precisely encryption processing in presentation layer) in the upper layers passes through securing the physical layer in optical networks. The reason this physical architecture of the fiber is responsible for the resources in terms of channel capacity and data rate that provide encryption and security of the fiber optical networks. Most of the attacks, in the physical layer of the optical networks composed of jamming, physical infrastructure attacks, and eavesdropping. To face those attacks many studies [23, 24] suggest optical encryption, optical code-division multiple access (CDMA)

confidentiality, self-healing survivable optical rings, anti-jamming, and optical steganography to handle the problem of the physical layer in the fiber networks.

There are many fiber-based mechanisms that effectively allow security for the optical network such as optical steganography [25–27], optical chaos-based communication [28–30], optical key distribution [31–33], and all-optical signal processing [34–36]. Fiber devices are resistant to electromagnetic interference. For example, the signal in fiber optics is not impacted by the electrical field and the interference that comes from thunder, high power transmission line. However, the electrical cable or line can be sensitive to static electricity and high-frequency electrical link. Some attacks based on jamming the fiber channel with electromagnetic waves cannot work. Optical networks are more secure compared with other networks based on the electrical cable because of their low latency and high data rate. Therefore, just using optical networks means that there is a low layer of security without negotiating its transmission speed. There are some studies that show securing the optical network increases the capacity of the channel instead of consuming the available resource. For instance, the optical key distribution [33] creates a separate and high secure channel to carry key data.

Implementing a security in any type of network requires looking at the Confidentiality, Integrity, Availability (CIA) triad, which is a model designed to guide policies for information security. In this section, we depict the optical steganography to ensure the privacy of optical networks. We also discuss the optical encryption and optical code-division multiple access (CDMA) to ensure the confidentiality. Finally, we examine the anti-jamming methods and optical chaos-based communication to ensure the availability of the communication network system.

2.2.2 Privacy and optical steganography. One of the components of the CIA of security is the confidentiality or privacy. It aims to prevent sensitive or private information from being reached by the wrong people and makes sure that the information will be received and transmitted to the right and authorized people [37]. Encryption is one way to ensure privacy by protecting the original data from being received by an attacker or eavesdropper. However, it cannot protect the existence of the encryption data in the channel. Some attackers, if they know that there is an encrypted channel, will try decrypting it. One solution to correct this issue is to hide the private channel or signal in the public cover channel so that any eavesdropper cannot see the existence of this private channel. This is called optical steganography [38–41]. The eavesdropper cannot detect the private signal (hidden in the stealth channel) because it buries this channel in the noise that already exists in the system. In time or spectral domain, there is no way to detect the existence of the hidden channel and the power of this hidden channel is lower than the public channel.

The first work that proposes and experiences the optical steganography mechanism is directed by Bernard Wu and his team [25]. Through the chromatic dispersion, the short pulse is spread and stretched. This optical stretching signal is hidden in the noise channel. The idea of this approach of the optical steganography is to create an optical cover channel by temporarily spreading the signal so that the average power will be lower than the noise floor existing in the public channel.

Optical steganography has been demonstrated using different types of modulation including return-to-zero (RZ) on-off-keying [42], non-return-to-zero (NRZ) [43], optical CDMA [44], and differential (quadrature) phase-shift keying (DPSK/DQPSK) [45]. To

improve the confidentiality of the stealth channel, we add a temporal phase mask shift to stretch the signal [46] by covering each stealth optical bit with a 16-chip phase. In this case, dispersion and the phase mask between transmitter and receiver should be matched to recover and demodulate data.

Optical steganography mechanism covers the stealth channel in a time domain until it becomes difficult to distinguish the signal with the noise. In the spectral domain, the stealth spectra merge with the noise especially when there is a high percentage of noise in the public channel. The issue of this steganographic method that is based on dispersion is that the shape of the noise spectrum is not the same as the ones in the stealth channel. This problem is addressed by using another optical steganography technique based on Amplified Spontaneous Emission (ASE) noise.

2.2.3 Confidentiality in the physical layer network. In the information security, data confidentiality is an important component of the CIA triad to ensure security. It makes sure that the data is transmitted to the right users and will not be disclosed by unauthorized users in the computer networking [37]. The eavesdropper can receive the residual crosstalk by listening from a co-site channel [47] or tapping the fiber optic [48]. Ensuring data confidentiality requires implementing optical encryption and optical coding in the physical layer network. Those mechanisms are resistant to electromagnetic radiation and interferences. There are many mechanisms to ensure the confidentiality of the optical physical layer including the optical encryption, optical CDMA as well as the key distribution for coding and encryption.

2.2.4 Availability in the physical layer network. One of the aspects of the CIA triad of security information is called availability. This approach makes sure that the optical network is available to authorized users and denied to unauthorized users. One big issue that impacts the availability of the optical network is the jamming of the channel by the noise. Optical steganography mechanism based on ASE noise will be a solution for the jamming of the channel. Thus, ensuring the availability of the network.

In this technique, the ASE noise is a C-band noise that carries the signal of interest in the optical communication. It means that the attacker will have a hard time carrying out malicious jamming. In case the adversary jams the entire C-band, there will be no more bandwidth channel left. Another approach to ensure the availability of the physical optical layer is using the waveband conversion technique. It can be implemented with a periodically-poled ($LiNbO_3$) material [49].

To overcome the malicious jamming, chaos-based communications provide a solution. It corrects band interference and jams the communication of attackers. The difference between optical steganography and optical chaos-based communication is that optical steganography reduces the amplitude of the hidden signal. However, chaos-bases communication masks confidential data with much chaos. Only the receiver knows how the chaos is generated so they can cancel it at the end to recover the signal. There are some researchers that demonstrated the optical chaos-based communications with high data rate about 1Gb/s and bit-error rates (BER) 10^{-7}[29]. For example, Argyris et al. transmit the optical chaos-signal over 120 km distance of optical network. The optical chaos signal is mostly generated by fiber loops and Erbium-doped fiber amplifier (EDFA) [30, 50].

2.3 Free Space Optical Communication Systems

2.3.1 Overview of free space optical (FSO) communication. Before giving definition of the free space optical (FSO) communication, we should define the optical wireless communication (OWC). Optical wireless communication refers to the transmission of the data in an unguided propagation channel using optical carriers such as visible, infrared (IR), and ultraviolet (UV) bands of the electromagnetic spectrum. If the OWC systems operate and use a visible band [390-750 nm], then we call those systems visible light communication (VLC) systems (Figure 8). Whereas, if we use the terrestrial point to point OWC systems with an infrared (IR) band [750-1600 nm], then we will talk about the free space optical (FSO) communication (Figure 9).

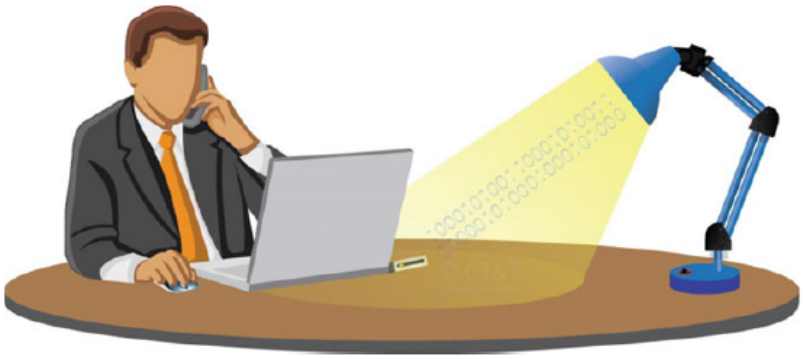

Figure 8. Example of the visible light communication system [51]

2.3.2 Advantages and applications of FSO. Free space optical communication (FSO) system represents a solution for the system that requires a high speed and a point to point transmission with a range up to several kilometers. Comparing with radio frequency

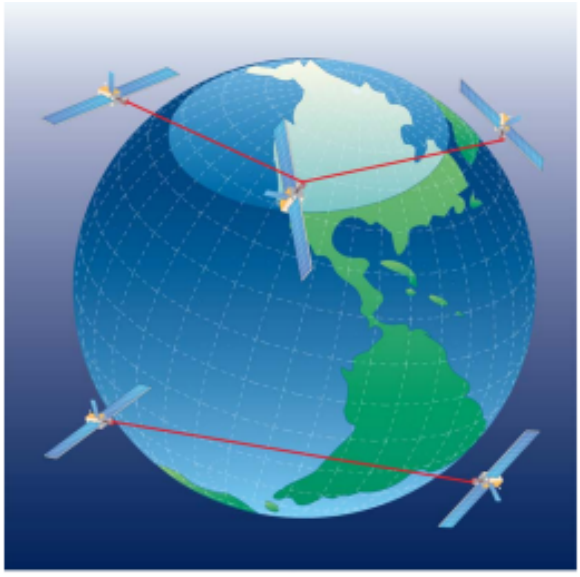

Figure 9. Example of the free space optical communication system [20]

(RF) link, the FSO channel offers a high optical bandwidth allowing it to have a much higher data rate and speed. Actually, the terrestrial OWC products or systems are available in the market with a data rate of 10 Gb/s [52]. Recently, the OWC systems compete with fiber optical communication systems [53, 54]. Most of the FSO communication systems use narrow laser beams to carry the information. This feature allows them to ensure inherent security, immunity against the interference, and a high reuse factor. Due to the use of high frequency (above 300 GHz) and unlicensed spectrum in FSO technology, the FSO systems don't need license fees [55]. Another advantage of the FSO is the easiness to deploy and it is economical because we don't need to install the fiber optic connections.

We can apply the FSO communication systems to different areas [20]:

1. Campus connectivity is one of the areas where the FSO may be deployed. Multiple buildings can be linked using FSO mechanism that provides a high data rate of

communication.

2. Video surveillance and monitoring is another area of FSO application. It is obvious that video streams require a high throughput, which conventional technologies in wireless communication fail to have. Therefore, FSO communication solves this problem by offering a high capacity.

3. Security is required for any communication system. FSO link offers a high level of secure communication especially when the fiber optic link is not feasible. Cryptography and steganography techniques are used for this purpose.

4. Disaster recovery is another domain of application of FSO. Occasionally, when disaster damages an area, the immediate FSO link is needed quickly.

5. Another domain of application is broadcasting and transmission to several receivers especially when there is a high viewership broadcasting event. The FSO link satisfies this need with a high definition and video quality.

Chapter 3

Stealth Optical Communication System Using an Amplified Spontaneous Emission Noise in Free Space

Our project is to build and demonstrate a practical and feasible optical communication system prototype that responds to three requirements: security, speed, and adaptability to the wireless communication system such a smart sensors networks. This custom built security network was analyzed and calculated for performance using eye diagram and bit-error rate (BER). This could have future applications for smart sensor networks. Using the steganography technique with ASE noise ensures the privacy of the communication system. The stealth (hidden) channel is not detectable by eavesdroppers. The optical communication provides a large bandwidth in comparison to RF communication, which means that the speed of the optical communication is higher in large scale compared with RF communication. Finally, transmission in unguided media (FSO link) offers a solution and a huge application for the optical wireless networks such as smart sensor networks.

3.1 Description of the Stealth Optical Communication System

The schematic of the stealth optical communication system that satisfies the three requirements above is given in Figure 10.

This design corresponds to the generic optical communication system that is traditionally composed of the transmitter, the channel of communication and the receiver. Let's describe each part of the system.

3.1.1 Stealth optical transmitter. The main components of the transmitter are the optical source, the modulator, and the optical amplifier. In our transmitter (Figure 11), the

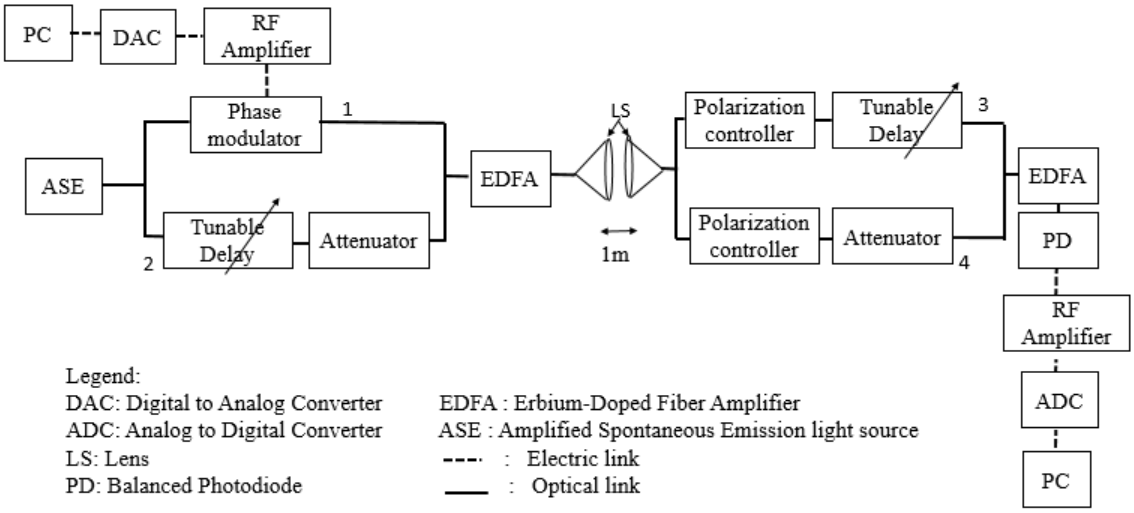

Figure 10. The schematic of the stealth optical communication system

optical source is the Amplified Spontaneous Emission (ASE). It is a source of light that produced by spontaneous emission. This source of light has been optically amplified by the process of stimulated emission in a gain medium. The modulator that we chose in this setup is the external phase modulator. Basically, it changes the pattern that encodes information as variations in the instantaneous phase of a carrier wave. The source of data is a stream of bits “0” and “1” generated by using a personal computer and digital-analog converter, which convert the signal in time domain to digital signal. To modulate the digital data in order to be converted in the optical domain, we need to amplify this digital data (RF signal). For this purpose, we use the RF amplifier that amplifies a radio frequency power. In the transmitter, we use two electronic devices tunable delay and the attenuator in order to get approximately the same optical power in two lines of the light path of the ASE noise. Tunable delay plays a role in the motorized variable optical delay line that provides precision optical path length adjustment. The attenuator attenuates the optical power that

is transmitted. The optical amplifier is an Erbium-Doped Fiber Amplifier (EDFA) that intensifies the power of the signal directly without the need of converting it to an electrical signal.

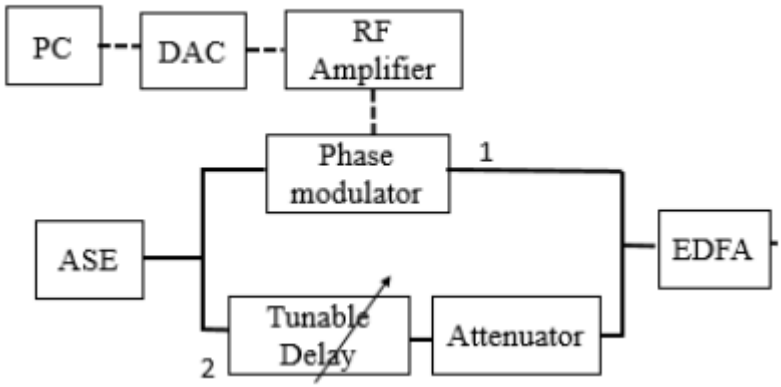

Figure 11. The schematic of the stealth transmitter (PC: personal computer; DAC: digital to analog converter; ASE: amplified spontaneous emission light source; EDFA: erbium-doped fiber amplifier)

3.1.2 Stealth transmission channel. In our system, the communication channel is an unguided channel when we transmit the optical signal from the transmitter to the receiver in the free space (air). It is the free space optical (FSO) link. Basically, this link is a point to point link with two lens in the extremity. Those two lenses are a transmissive optical device that focuses a light beam by means of refraction.

3.1.3 Stealth receiver. The main elements or traditional optical is the demodulator and the photodetector. In our setup (Figure 12), the photodetector is the photodiode (PD). It is the receiver in the optical communication system. This device converts the optical

light to the electric signal. For the demodulator, we just use a mechanism called homodyne detection (see above to understand this technique) to extract the data signal. A tunable delay and attenuator are required to keep the same optical power in both lines of the receiver. EDFA amplifies the optical signal in order that the photodiode detects and converts it to an electrical signal that will be amplified by the RF amplifier. We have two polarization controllers in both lines paths of the receiver. Their goals are modifying the polarization state of the beam light. The analog-digital converter (ADC) converts the digital bits into the analog data signal which we can see in the personal computer (PC).

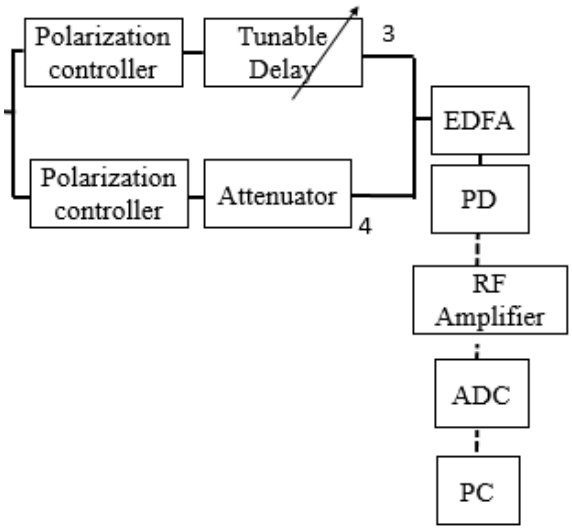

Figure 12. The schematic of the stealth receiver (EDFA: erbium-doped fiber amplifier; PD: photodiode; ADC: analog to digital converter; PC: personal computer)

3.2 The Operation of the Stealth Communication

We transmit 500 Mb/s of private data from the couple PC and DAC. In our experiment, the use of the HP 70841b pattern generator, HP 70842b error detector ,and HP 70004A Graphics Display were recommended. First, they generate 500 Mb/s of the data

by HP 70841b pattern generator. Second, the display was detected in the shape of the eye diagram by using HP 70004A Graphics Display. Lastly, the bit-error rate (BER) of our system was calculated via the HP 70842b error detector.

In this system setup, PC and DAC are equivalent to the three HP module. This generator generates eye pattern (eye diagram) with the frequency of 500 MHz . This data generated by eye diagram (Figure 13) represents a respective samples of “0” and “1” bits.

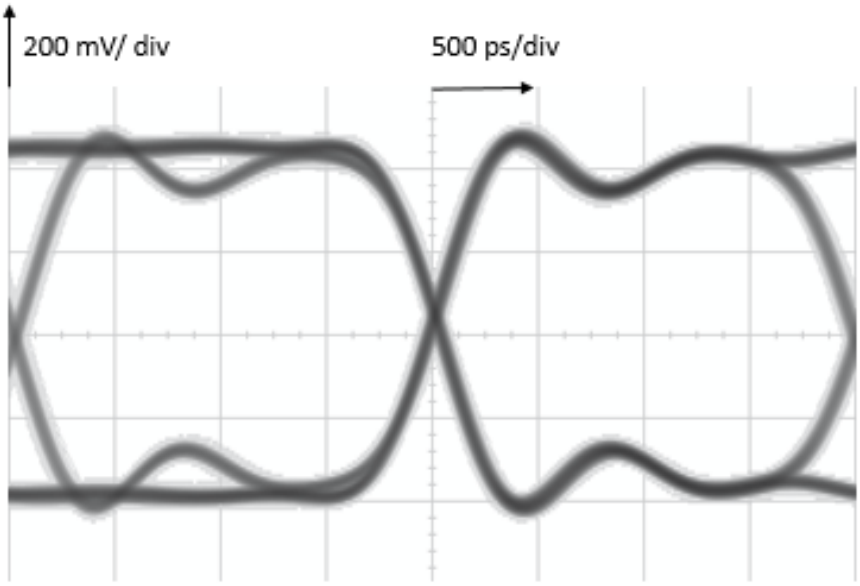

Figure 13. Eye diagram of 500 Mb/s transmitted data

To modify this data and put it in the optical channel, it is preferable to amplify this eye diagram in term of intensity (we use the RF amplifier for this purpose).This private data is carried by a wide C-band optical signal generated by the amplified spontaneous emission (ASE) light source. This ASE generates a c-band spectrum with an optical power of the 52.8 mW which corresponds to 17.23 dBm using the following formula:

$$P(dBm) = 10 \times \log 10 \frac{P(mW)}{1mW} \tag{3.1}$$

To see the bandwidth of this source light, we connect this devise ASE-C light source with the optical spectrum analyzer using the single fiber optic. The output of the optical signal is in the Figure (14).

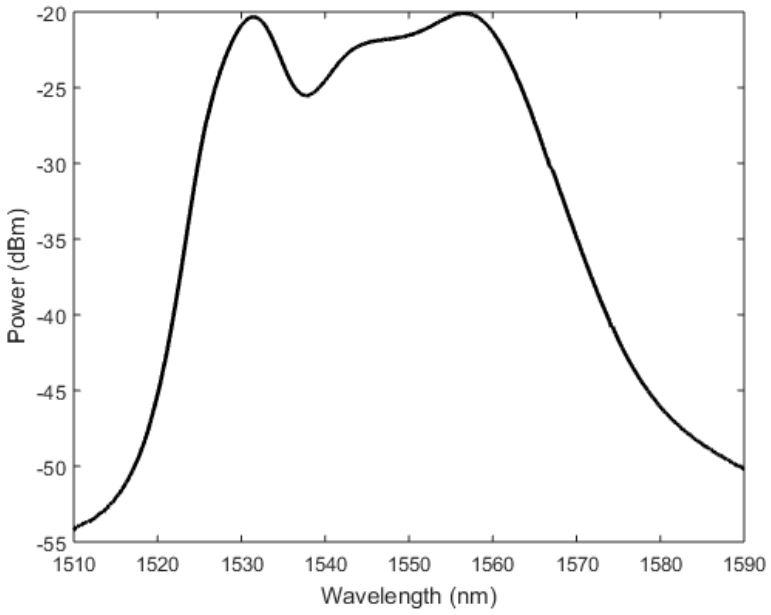

Figure 14. Optical spectrum of the ASE

The source of the light that carried the private data of 500Mb/s is a C-band with a wide bandwidth between λ_1 = 1530 nm and λ_2 = 1556 nm. It corresponds to f_1 = 196 THz and f_2 = 192 THz. The bandwidth of the optical ASE light beam is $\triangle f$ = f_1-f_2 = 4 THz. The optical signal is split into two beams light using a splitter and the following two paths are : The upper beam light carries our private data after phase modulation. The bottom part of the beam light enters to tunable delay and attenuator. The logic behind adding attenuator

and tunable delay is to get the same optical power in both split channels in which will be added using a combiner. The next step will be using the Erbium-Doped Fiber Amplifier (EDFA) amplifying the optical signal, and to compensate the loss and transmit the optical signal through FSO channel.

At the receiver side, the same process occurred. We split the optical signal and divide it into two parts. First part is entered into controller polarization and tunable delay, and the second one entered into attenuator and controller polarization. Afterward, two signals are combined and amplified to detect the private data using the balanced photodiode. The photo diode translates the optical signal into the electric signal that will be amplified to be detected and displayed in HP 70004A Graphics Display which equivalent to use the ADC and PC. It is important to notice that at the receiver side, the two beams light that across two paths should have to same optical power in order to interfere and be combined. Another point to mention is that our optical communication system follows a structure of MZ interferometer in order to extract the private data at the receiver side using homodyne detection. In our optical communication system, we reach a 4 THz bandwidth of the amplified spontaneous emission (ASE) source that carries the 500 Mb/s private data. It means that we transmit the private data with a data rate of 4 Tb/s.

3.3 Analog Steganography of the System

Our optical communication system is secure because it protects the privacy data underneath of the ASE noise generated by the source light and the optical amplifier EDFA. Those two ASE have the same feature. The hidden data is called also stealth data. This is called steganography mechanism. As we said above the structure of the stealth channel

that is composed of the stealth transmitter and stealth receiver is MZ interferometer. The short coherence length of the ASE noise is the one important key that prevents the data to be extracted. The stealth signal is hidden using a DPSK phase modulator in one arm of the interferometer. In this experiment, we use the C-band of the ASE noise. The combination of both public and stealth transmitter is done by a combiner, and amplified by the EDFA to send over 1m of the FSO link. The beam light coming from the ASE source light take two paths: path $1 \rightarrow 3$, $2 \rightarrow 4$ or path $1 \rightarrow 4$, $2 \rightarrow 3$ (Figure 10).

In this experiment, the length of line 1 is 2m longer than line 2. The interference between the two beams that passing different paths occurs when the length of one pair of the light match with other part, and it happens exactly when the optical length difference is within the short coherence length of the ASE noise, which is about 312 μm (see Results and Analysis) in this experience. In this setup, two tunable delay lines are used. One in line 2 and the other is in line 3 at the stealth receiver. To make the task harder for an eavesdropper to detect the private information, they use two computers to control those two tunable delays. The tunable delay line 3 follows the movement of the tunable delay line 2 to mimic the movement of the position in order to get the matching condition.

3.4 Results and Analysis

3.4.1 Coherence length measurement. It is important to explain how this setup arrives to measure the coherence length of the ASE noise. Basically, we try to reach the matching condition between two beams light path to interfere and then calculate the coherence length of the ASE. More specific, we scan one of the two delay lines and use the photodiode at the receiver to detect the output power. If the optical delay length difference

between the path $1 \rightarrow 3$, $2 \rightarrow 4$ is longer than the coherence length of the ASE, that means that there is no interference between those two paths leading and having a constant power at the detector. On the other hand, if the optical length difference is within the coherence length, the interference will be noticed by a change in the received power at the detector. And in this case, the matching condition is reached and the interference peak is observed at the detector (Figure 15). This figure is done by measuring two variables optical delay and the intensity of the optical signal at the receiver. We got a data of 600 rows and 2 columns corresponding to the optical delay and the intensity of the optical delay.

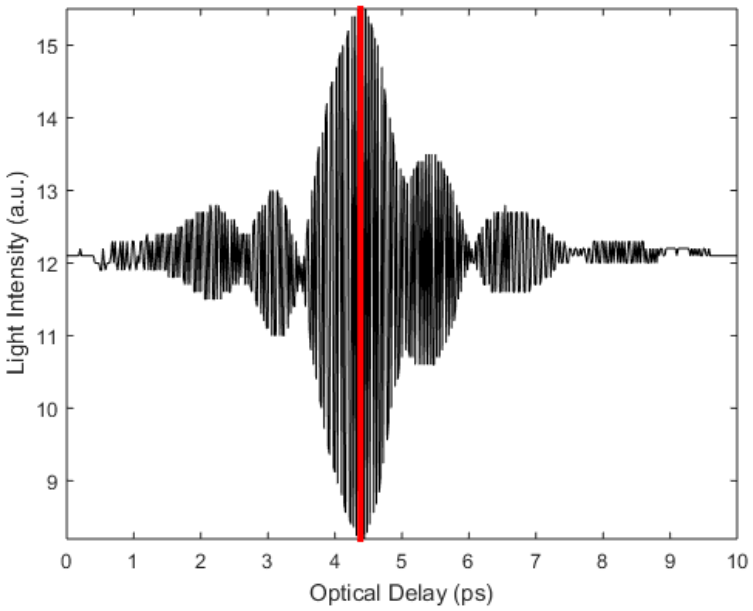

Figure 15. Matching condition

To determine the duration of the optical delay which two light beams match, we calculate what is called the full width at half maximum (FWHM). This value is an expression of the extent of a function given by the difference between the two extreme values of

Table 2

Different values of the optical power with different values of the wavelengths

Wavelength(nm)	1510	1510.2	1510.3	1510.5	1510.6
Power(dBm)	-57.515	-57.536	-57.543	-57.559	-57.591

the independent variable at which the dependent variable is equal to half of its maximum value.

By measuring the full at half-maximum (FWHM) of the interference peak, which is about 1.04 ps, we can get the coherence length of the ASE noise which is 312 μm in optical length.

The spectrum of the ASE noise is calculated after the output of the optical amplifier EDFA at the receiver. The data from the spectrum analyzer connected to the output of the EDFA at the receiver was measured. We got 501 values of the wavelength and the optical power correspondent using a function in Matlab and the cable GPIB. The first 5 data of our spectrum is shown in Table 2.

Figure 16 shows the spectrum of the ASE noise at the receiver measured after the EDFA amplifier.

3.4.2 Hidden signal in the ASE noise. These results illustrate that the stealth channel cannot be detected. In the time domain, the eavesdropper receives only the constant power if he tries to listen directly from a transmission line (see Figures 17(a), 17(b)). The Figure 17(b) shows that when the signal or data is sent in no matching condition, we got a constant power at the receiver. So, the eavesdropper can't detect the signal because he does

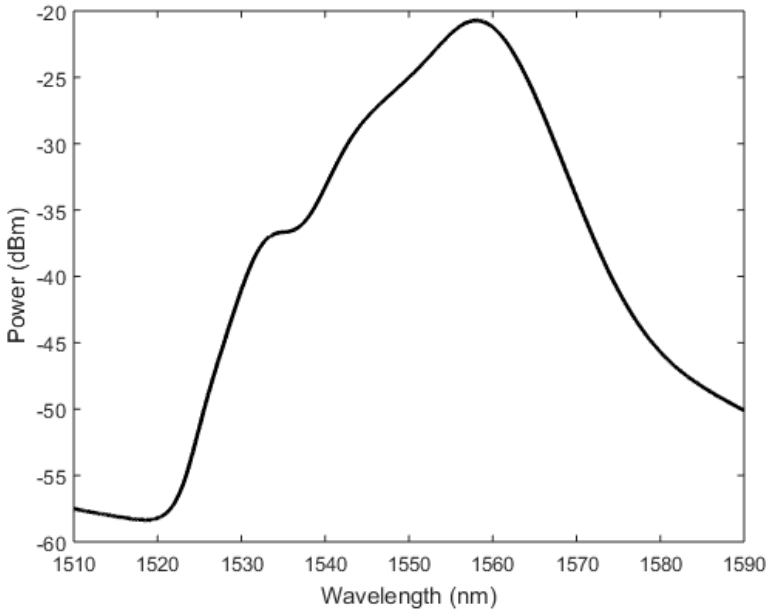

Figure 16. The optical spectrum of the ASE measured after EDFA

not know the matching condition which is the key to the steganography mechanism using ASE noise. The Figure 17(a) shows that when the signal is off (not sent) at the matching condition, we got also a constant power at the receiver. Those two figures show that we create and transmit a stealth channel over ASE noise in the free space transmission channel. At matching condition and when the signal is on and sent to the transmission line, we got a clear eye diagram (Figure 17 (c)).

3.4.3 The Bit error rate (BER) measurement. As we said in chapter 2, the BER is considered a metric to measure the performance of the optical communication system. In our system, we calculate the received power at the receiver in matching condition, and we record the BER and the display of eye diagram corresponding. At the receiver, we add a loss to decrease the power and record the BER. Table 3 shows those measurements for 5

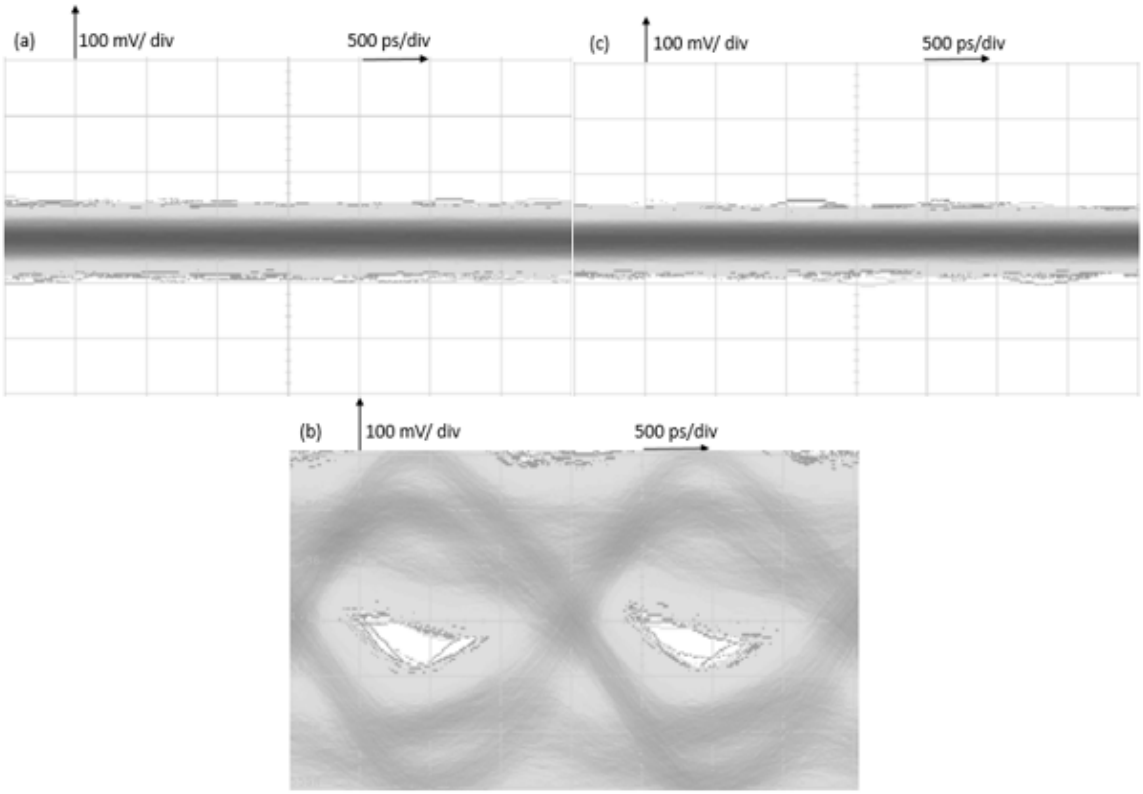

Figure 17. Demonstration of the stealth channel in time domain. (a) Signal off at matching condition . (b) Signal on at matching condition. (c) Signal on at no matching condition.

Table 3

Bit-error rate (BER) of the system in logarithm scale

Received power (dBm)	9.69	8.68	7.67	6.66	5.69
Log10 (BER)	-5.3585	-5.2757	-5.1343	-5.0788	-4.9931

records. At matching condition, we expect to have a minimum of the BER, especially when the interference peak is reached. This is the output of the BER (Figure 18) in function of the received power.

The Figure 19(a) shows the Eye diagram at lower power. In this case, the diagram is

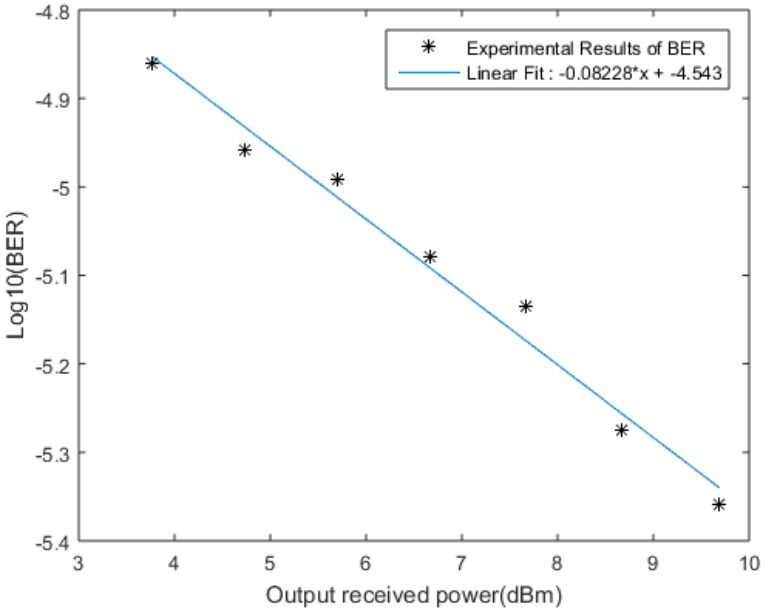

Figure 18. The BER of the stealth communication system

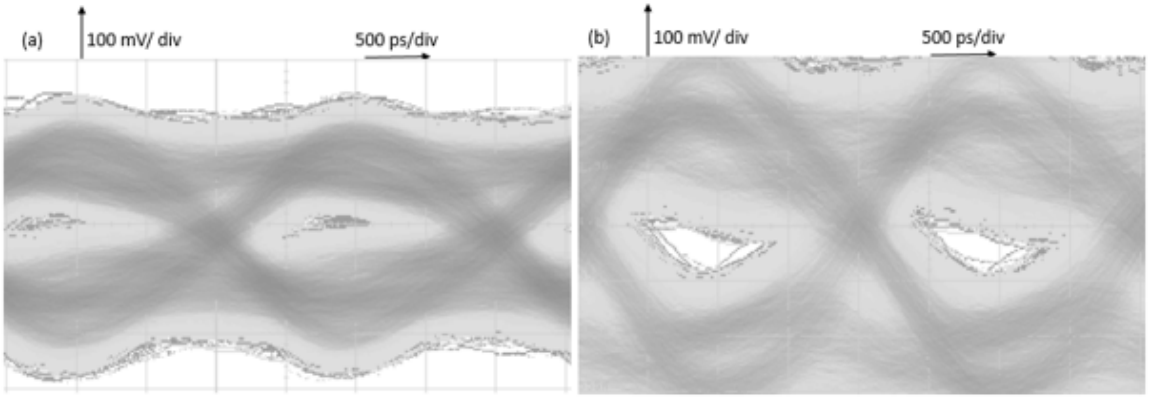

Figure 19. (a) Noisy eye diagram corresponding to less received power. (b) Clear eye diagram corresponding to more received power

a noisy eye, which corresponds to the high value of BER. The Figure 19(b) the eye diagram at higher power. For this case, the eye diagram has a clear eye, which corresponds to the less value of BER.

Chapter 4

Conclusion and Future Work

This thesis has been demonstrating experimentally a secure optical communication system using an amplified spontaneous emission noise in free space that can be applied to new technologies such as internet of things and smart sensors networks. It also measures the performance of this system using eye diagram and bit-error rate. For security (privacy and availability), we use the steganography mechanism, which is based on hidden information (stealth channel) underneath a cover or public channel (ASE noise). We ensure to transmit a large scale of data using optical communication instead of RF communication. Free space offers an economical and practical solution especially when the fiber channel can't be deployed. FSO offers unlicensed spectrum, easiness to deploy and adaptable for cyber-physical systems. In conclusion, we demonstrated the analog steganography based on ASE noise that allows hiding the stealth signal underneath c-band noise. We ensured a high data rate of the communication system by using the huge optical spectrum that carries the private data. Finally, we implemented this system in free space (FSO) channel to transmit the data to use it for new smart networks and various applications.

4.1 Summary of Future Work

Further work is needed to add another layer of security in this optical communication by combining optical steganography with optical encryption. Since we know how to build a secure optical communication system point-to-point, we will go further by building a single in multiple outputs (SIMO) secure optical communication system in free space. We propose to use a digital micromirror (DMD) in free space (FSO) link to direct light

beams to different directions of receivers. This device can help to achieve a control of the phase amplitude matching condition for moving receivers. This work can be used in the various applications such as smart sensor networks application.

References

[1] Edward A. Lee. Cyber physical systems: Design challenges. In *Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing*, pages 363–369, 2008.

[2] Md.E Karim and Vir.V Phoha. Cyber-physical systems security. In *Applied Cyber-Physical Systems*, pages 75–83. Springer, 2014.

[3] Joseph Mitola Iii. An integrated agent architecture for software defined radio, 2000.

[4] J. Mitola and G. Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, 1999.

[5] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, 2005.

[6] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys Tutorials*, 11(1):116–130, 2009.

[7] J. Mitola. 1999cognitive radio for flexible mobile multimedia communications. In *Mobile Multimedia Communications, 1999. (MoMuC '99) 1999 IEEE International Workshop on*, pages 3–10, 1999.

[8] L. Cimini. Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing. *IEEE Transactions on Communications*, 33(7):665–675, 1985.

[9] Yiyan Wu. Orthogonal frequency division multiplexing: A multi-carrier modulation scheme. In *Proceedings of International Conference on Consumer Electronics*, pages 8–, 1995.

[10] B. Le Floch, M. Alard, and C. Berrou. Coded orthogonal frequency division multiplex [tv broadcasting]. *Proceedings of the IEEE*, 83(6):982–996, 1995.

[11] Richard DJ Van Nee. Orthogonal frequency division multiplexing system with dynamically scalable operating parameters and method thereof, January 16 2001. US Patent 6,175,550.

[12] Rajiv Laroia, Junyi Li, and Michaela Catalina Vanderveen. Orthogonal frequency division multiplexing based spread spectrum multiple access, October 29 2002. US Patent 6,473,418.

[13] V Zarzoso and AK Nandi. Blind source separation. In *Blind Estimation Using Higher-Order Statistics*, pages 167–252. Springer, 1999.

[14] Adel Belouchrani, Karim Abed-Meraim, J-F Cardoso, and Eric Moulines. A blind source separation technique using second-order statistics. *IEEE Transactions on signal processing*, 45(2):434–444, 1997.

[15] J-F Cardoso. Infomax and maximum likelihood for blind source separation. *IEEE Signal processing letters*, 4(4):112–114, 1997.

[16] Michael Zibulevsky and Barak A Pearlmutter. Blind source separation by sparse decomposition in a signal dictionary. *Neural computation*, 13(4):863–882, 2001.

[17] Pau Bofill and Michael Zibulevsky. Underdetermined blind source separation using sparse representations. *Signal processing*, 81(11):2353–2362, 2001.

[18] B. Wu and Y. Ergaibi. Optical stealth communication for smart sensor networks. In *2017 IEEE Sensors Applications Symposium (SAS)*, pages 1–5, 2017.

[19] Govind P Agrawal. *Fiber-optic communication systems*, volume 222. John Wiley & Sons, 2012.

[20] Mohammad Ali Khalighi and Murat Uysal. Survey on free space optical communication: A communication theory perspective. *IEEE Communications Surveys & Tutorials*, 16(4):2231–2258, 2014.

[21] Yang Ji, Yunchul Chung, D Sprinzak, M Heiblum, D Mahalu, and Hadas Shtrikman. An electronic mach–zehnder interferometer. *Nature*, 422(6930):415, 2003.

[22] Hubert Zimmermann. Osi reference model–the iso model of architecture for open systems interconnection. *IEEE Transactions on communications*, 28(4):425–432, 1980.

[23] Mable P Fok, Zhexing Wang, Yanhua Deng, and Paul R Prucnal. Optical layer security in fiber-optic networks. *IEEE Transactions on Information Forensics and Security*, 6(3):725–736, 2011.

[24] Ben Wu, Bhavin J Shastri, and Paul R Prucnal. Secure communication in fiber-optic networks. In *Emerging trends in ICT security*, pages 173–183. Elsevier, 2014.

[25] Bernard B Wu and Evgenii E Narimanov. A method for secure communications over a public fiber-optical network. *Optics express*, 14(9):3738–3751, 2006.

[26] MP Fok and PR Prucnal. Compact and low-latency scheme for optical steganography using chirped fibre bragg gratings. *Electronics letters*, 45(3):179–180, 2009.

[27] Ben Wu, Zhenxing Wang, Yue Tian, Mable P Fok, Bhavin J Shastri, Daniel R Kanoff, and Paul R Prucnal. Optical steganography based on amplified spontaneous emission noise. *Optics express*, 21(2):2065–2071, 2013.

[28] Gregory D Vanwiggeren and Rajarshi Roy. Communication with chaotic lasers. *Science*, 279(5354):1198–1200, 1998.

[29] Apostolos Argyris, Dimitris Syvridis, Laurent Larger, Valerio Annovazzi-Lodi, Pere Colet, Ingo Fischer, Jordi Garcia-Ojalvo, Claudio R Mirasso, Luis Pesquera, and K Alan Shore. Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature*, 438(7066):343, 2005.

[30] Lingzhen Yang, Li Zhang, Rong Yang, Li Yang, Baohua Yue, and Ping Yang. Chaotic dynamics of erbium-doped fiber laser with nonlinear optical loop mirror. *Optics Communications*, 285(2):143–148, 2012.

[31] Danna Rosenberg, Jim W Harrington, Patrick R Rice, Philip A Hiskett, Charles G Peterson, Richard J Hughes, Adriana E Lita, Sae Woo Nam, and Jane E Nordholt. Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters*, 98(1):010503, 2007.

[32] Robert H Hadfield, Jonathan L Habif, John Schlafer, Robert E Schwall, and Sae Woo Nam. Quantum key distribution at 1550 nm with twin superconducting single-photon detectors. *Applied physics letters*, 89(24):241129, 2006.

[33] Jacob Scheuer and Amnon Yariv. Giant fiber lasers: A new paradigm for secure key distribution. *Physical Review Letters*, 97(14):140502, 2006.

[34] Kerry Vahala, Roberto Paiella, and Guido Hunziker. Ultrafast wdm logic. *IEEE Journal of Selected Topics in Quantum Electronics*, 3(2):698–701, 1997.

[35] Kit Chan, Chun-Kit Chan, Lian Kuan Chen, and Frank Tong. Demonstration of 20-gb/s all-optical xor gate by four-wave mixing in semiconductor optical amplifier with rz-dpsk modulated inputs. *IEEE Photonics Technology Letters*, 16(3):897–899, 2004.

[36] Zhenxing Wang, Mable P Fok, and Paul R Prucnal. Physical encoding in optical layer security. *J Cyber Secur Mobility*, pages 83–100, 2012.

[37] William Stallings. *Cryptography and network security: principles and practice*. Pearson Education India, 2003.

[38] Paul R Prucnal, Mable P Fok, Konstantin Kravtsov, and Zhenxing Wang. Optical steganography for data hiding in optical networks. In *Digital Signal Processing, 2009 16th International Conference on*, pages 1–6. IEEE, 2009.

[39] Bernard B Wu, Paul R Prucnal, and Evgenii E Narimanov. Secure transmission over an existing public wdm lightwave network. *IEEE photonics technology letters*, 18 (17):1870–1872, 2006.

[40] Bernard B Wu and Evgenii E Narimanov. Analysis of stealth communications over a public fiber-optical network. *Optics express*, 15(2):289–301, 2007.

[41] Xuezhi Hong, Dawei Wang, Lei Xu, and Sailing He. Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering. *Optics express*, 18(12):12415–12420, 2010.

[42] Bernard Wu, Anjali Agarwal, Ivan Glesk, Evgenii Narimanov, Shahab Etemad, and Paul R Prucnal. Steganographic fiber-optic transmission using coherent spectral-phase-encoded optical cdma. In *Conference on Lasers and Electro-Optics*, page CFF5. Optical Society of America, 2008.

[43] K Kravtsov, B Wu, I Glesk, PR Prucnal, and E Narimanov. Stealth transmission over a wdm network with detection based on an all-optical thresholder. In *Lasers and Electro-Optics Society, 2007. LEOS 2007. The 20th Annual Meeting of the IEEE*, pages 480–481. IEEE, 2007.

[44] Y-K Huang, B Wu, I Glesk, EE Narimanov, T Wang, and PR Prucnal. Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques. *Electronics Letters*, 43(25):1449–1451, 2007.

[45] Zhenxing Wang and Paul R Prucnal. Optical steganography over a public dpsk channel with asynchronous detection. *IEEE Photonics Technology Letters*, 23(1):48–50, 2011.

[46] Z Wang, MP Fok, L Xu, J Chang, and PR Prucnal. Improving the privacy of optical steganography with temporal phase masks. *Optics express*, 18(6):6079–6088, 2010.

[47] Marija Furdek, Nina Skorin-Kapov, Marko Bosiljevac, and Zvonimir Šipuš. Analysis of crosstalk in optical couplers and associated vulnerabilities. In *MIPRO, 2010 Proceedings of the 33rd International Convention*, pages 461–466. IEEE, 2010.

[48] Keith Shaneman and Stuart Gray. Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention. In *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*, volume 2, pages 711–716. IEEE, 2004.

[49] Zhenxing Wang, Aref Chowdhury, and Paul R Prucnal. Optical cdma code wavelength conversion using ppln to improve transmission security. *IEEE Photonics Technology Letters*, 21(6):383–385, 2009.

[50] Henry DI Abarbanel, Matthew B Kennel, Michael Buhl, and Clifford Tureman Lewis. Chaotic dynamics in erbium-doped fiber ring lasers. *Physical Review A*, 60(3):2360, 1999.

[51] Murat Uysal, Carlo Capsoni, Zabih Ghassemlooy, Anthony Boucouvalas, and Eszter Udvary. *Optical wireless communications: an emerging technology*. Springer, 2016.

[52] D Rodewald. Mrv introduces industrys first 10g ethernet wireless point-to-point system. *MRV Communications, Inc*, 2008.

[53] Moon-Cheol Jeong, Jong-Seob Lee, Sang-Yuep Kim, Song-Won Namgung, Jae-Hoon Lee, Min-Young Cho, Suk-Woo Huh, and Jae-Seung Lee. 8x10 gb/s terrestrial optical free space transmission over 3.4 km using an optical repeater. In *Optical Fiber Communication Conference*, page ThD4. Optical Society of America, 2002.

[54] Shuailong Zhang, Scott Watson, Jonathan JD McKendry, David Massoubre, Andrew Cogman, Erdan Gu, Robert K Henderson, Anthony E Kelly, and Martin D Dawson. 1.5 gbit/s multi-channel visible light communications using cmos-controlled gan-based leds. *Journal of lightwave technology*, 31(8):1211–1216, 2013.

[55] Vincent WS Chan. Free-space optical communications. *Journal of Lightwave technology*, 24(12):4750–4762, 2006.