Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 11 November 2022

Research Article

Ways to Achieve Secrecy in the Optical Fiber Wiretap Channel

Mohammad Reza Deylam Salehi[1]* and Hassan Tavakoli[2]

[1]*Communication Systems, Eurecom, France*

[2]*Electrical Engineering, University of Guilan, Iran*

***Corresponding Author:** Mohammad Reza Deylam Salehi, Communication Systems, Eurecom, France.

Received: September 25, 2022

Published: October 12, 2022

Abstract

Through the use of optical fibers, we attempted to demonstrate a particular type of wiretap channel. Wiretap channels utilizing optical fibers are discussed with a focus on the distance between users in order to improve channel secrecy. To achieve this goal, we determine a measurement for the distance between the legitimate receiver, sender, and eavesdropper to ensure security by using wiretap channel error probability and link length attenuation in the wiretap channel's capacity equation. Moreover, we investigate the different types of optical receivers, the Positive-Intrinsic Negative (PIN) and the Avalanche Photo Diodes (APD), comparing their ratios over different load resistances and considering resistance as a key parameter for both sides to improve or decrease secrecy. The relationship between load resistance of legitimate receiver and eavesdropper was also driven using separate optical receivers for legitimate receiver and eavesdropper following the PIN and ADP optical receivers.

Keywords: Wiretap Channel; Optical Fiber; Error Probability; Attenuation

Introduction

Optical communication goes back as far as the Roman times, which use glasses for communicating along ships with lighthouse sea. The idea of communicating with light wave was extended by a suggestion of Claude Chappe in 1792, in order to transmit a mechanically encoded message over long distance ($\sim 100km$) by using intermediate relay stations [1].

The advent of telegraphy in the 1830s change the use of light with electricity and start an era of electrical communications [2]. In the middle of the twentieth century, many orders of magnitude in Bell Lab products would be achieved by using optical waves as the carrier. However, there were some problems such as they were no coherent optical source and no suitable transmission medium was available during the 1950s. The invention of the laser in 1960 [3] solved the problem of coherent optical source and introducing optical fibers in 1966s solved the second problem. They find out optical fibers might be the best choice [4], as they were guiding the light in the same way of electrical in copper wires.

Even though, the fiber-optic communication technology is new, it has progressed rapidly and has reached a certain stage maturity. This progress increases the necessity of secrecy in transmitting data in optical fiber.

In this paper, we simulate the wiretap channel by implementing the channel links by optical fiber. Then, by using the information theory rules for wiretap channel, we try to set some rules on optical fibers to fulfill wiretap channel rules in this media.

The paper presented as follows; in Section II, some preliminaries were presented. Section III discusses Optical fibers wiretap channel with the PIN. And wiretap with APD and conclusion is presented in Section IV and V.

Preliminaries

Wiretap channel

The Wiretap Channel, that illustrates in Figure.1, first presented by Wyner in an article by Bell Labs in 1975 [5]. In this channel, a legitimate transmitter (Alice) wishes to send a secure message through a channel to the legitimate receiver (Bob) while wiretapper (Eve) eavesdrop. The main issue in this channel is to prevent eavesdropper to have knowledge about information transmitted between sender and receiver. The channel between legitimate sender and receiver called the main channel, also the channel between eavesdropper and sender called wiretapper channel [6].

Figure 1: Wiretap Channel.

Two parameters needed for defining the capacity of a wiretap channel. The first one is Rate and another one is equivocation rate this pair called as equivocation pair. We use this pair as a measure for secrecy [7].

Equivocation rate for a wiretap channel define as bellow in this equation present a message that we send, represent the message that Alice wishes to send and decoded version in Eve side. In this article we use a discrete memoryless wiretap channel consist of a finite input alphabet X and two finite output alphabets Y & Z . A $(2^{nR},n)$ code C_n for a DWTC consist of a message $W=[1,2^{nR}]$ and an encoder function $f:W\times R\to X^n$ and decoding function $g:Y^n\to W\cup\{?\}$ which maps each observation to a message an error message ?.

$$R_e=\frac{1}{n}H(W^n|Z^n) \quad \text{----------(1)}$$

And rate for wiretap channel define as follows:

$$R=\frac{1}{n}H(W^n|Y^n) \quad \text{----------(2)}$$

The capacity region of the wiretap channel, introduce by Csiszár, Korner [8] for the first time as follows:

$$c(W)=\left\{\begin{array}{c}(R_e,R)\\ 0\le R\le c(m)\\ 0\le R_e\le R\\ R_e\le c(m)-c(w)\end{array}\right\} \quad \text{----------(3)}$$

We sketch the capacity region from their achievement. In their work, wiretap channel divided to two different channels. The first channel called the main channel and the other name as wiretapper channel we show the capacity of these channels by C_m and C_w as below.

Figure 2: Capacity region of wiretap.

We also define secrecy capacity for wiretap channel as follows:

$$C_s=\max_{P_x} I(X,Y) \quad \text{----------(4)}$$

Optical fiber

The advent of telegraphy in the 1830s replaced the use of light by electricity and began the era of electrical communication [2]. The phenomenon of total internal reflection for guiding light wave in optical fibers has been known since 1854 [9]. Also, glass fibers were made in 1920s [10-12]. Their use became more common only in the early 1950s when by some changes in the cladding layer, they improve the guiding characteristic of optical fibers was improved [13,14].

Because of suddenly changing in index value at the core-cladding interface, such fibers are called step-index fibers. The other type of fiber. Are known as graded index fibers, the reflecting index decreases gently inside the core [9].

Figure 3: Fiber Type based on Reflection Index.

PIN Photodiodes are as same as the p-n junction and use to detect optical wave. The technique that they use in the PIN to increase depletion-region width is to insert a layer of undoped semiconductor material, between p-n junction. Since the middle layer consists of nearly intrinsic material, such a structure is called the PIN photodiodes.

APD, Avalanche photodiode, have a much larger value of R, as they are designed to provide an internal current gain photomultiplier tube.

The difference between PIN an APD receivers is from an extra layer that adds into APD which secondary electron-hole pairs are generated through impact ionization.

The design of an optical receiver depends on the modulation format that transmitter used in this case (Alice) since most light wave systems employs the binary intensity modulation.

The structure of a receiver shows in the figure below.

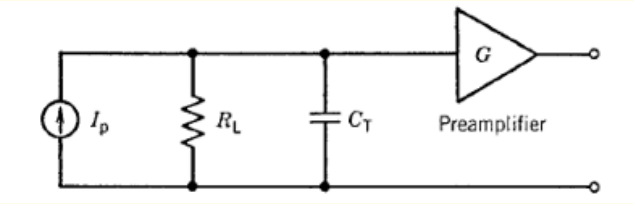

Figure 4: Receiver structure.

Optical fiber wiretap channel with PIN

Pervious work

Secrecy issues in the transmission of data made researchers to discuss every scenario that enemy can reach our message. These scenarios also include optical media for transmitting data. In [15] secrecy issues of the free-space optical link and realizing secure communication and higher data rates are discussed, they showed that information transmitting security under some degraded conditions on wiretapper, should be possible in the wider distance.

The physical-layer security of line of sight (LOS) free-space optical (FSO) link by using orbital angular momentum (OAM) multiplexing was studied, and power cost effect at the transmitter side for fixed power in the system and equal channel power discussed in [16]. In [17], by considering that near optical band communication is more secure than comparable RF channels because of their narrow-band beam-widths and high atmospheric absorption some coding techniques were discussed to combat wiretapping in these channels.

Authors in [18], proposed a method for optimizing information theoretic secure valuable input of a MIMO degraded wiretap channel using inverse preceding in order to evaluate the secrecy capacity on their method.

Also, in [19] hence the recent development in space-division multiplexing (SDM) for fiber-optic communication system suggest a spatial diversity by SDM that can use not only for improvement in capacity but also achieve secrecy improvement against physical layer attacks. That includes wiretap channel. And the more practical article in optical sensors to protection on objects such as pipelines. And the author compares their design by object security that available in the market [20].

The physical layer security investigated in [21]. Authors focused mainly on space division multiplexing to achieve information theoretical provable way against what their called fiber-tapping.

More recently, research in this field was carried out by Soltani and Rezki in [22]. They considered an optical wiretap channel with input-dependent Gaussian noise. In this article, we tried to focus on optical fiber and discuss the issue, by using one of our pervious works [23].

Implementation of wiretap channel by optical fiber

In our model for the Wiretap channel, there is a main route namely the main channel and a Wiretapper channel for implementing this scenario. Know that in our model for wiretap

channel we have the main route. We use optical fiber for each of these links. For constructing these channels, we must consider some rules to simulate these fibers as wiretap channel, in wiretap channel from (3) we know that.

$$c(W)=\begin{Bmatrix}(R_e,R)\\0\le R\le c(m)\\0\le R_e\le R\\R_e\le c(m)-c(w)\end{Bmatrix} \quad \text{---------- (5)}$$

And we also know that the main channel in wiretap has less error probability than the wiretapper channel. The figure of our work illustrates as below.

Figure 5: Optical Fiber Wiretap.

The wiretapper channel, experience more attenuation than the main channel. in this section, we try to find a coefficient between the length of wiretap's main channel and wiretapper channel. To achieve this goal first, we introduce attenuation in optical fibers.

If we consider P_{in} as power launched at the input of transmitter, with fiber with length L, the output power P_{out} is given by:

$$P_{out}=P_{in}\exp(-\alpha L) \quad \text{---------- (6)}$$

It is common to express α in dB/km by using equation above we have:

$$\alpha(dB/km)=-\frac{10}{L}\log_{10}(\frac{P_{out}}{P_{in}}) \quad \text{---------- (7)}$$

In our scenario we want to find relation between two distances.

Main channel:

$$\alpha_m(dB/km)=-\frac{10}{L_m}\log_{10}(\frac{P_{out1}}{P_{in}}) \quad \text{---------- (8)}$$

Wiretapper channel:

$$\alpha_w(dB/km)=-\frac{10}{L_w}\log_{10}(\frac{P_{out2}}{P_{in}}) \quad \text{---------- (9)}$$

In addition to constructing wiretap channel, main link attenuation should be lesser than the wiretapper link.

$$\alpha_m<\alpha_w \quad \text{----------(10)}$$

From this equation we have:

$$L_w>L_m(\frac{\log\frac{P_{out2}}{p_{in}}}{\log\frac{P_{out1}}{p_{in}}}) \quad \text{----------(11)}$$

If we use PIN receivers for detecting and receiving data on both sides. We have BER (Bit Error Rate) as follows:

$$BER=\frac{1}{4}\left[erfc(\frac{I_1-I_D}{\sigma_1\sqrt{2}})+erfc(\frac{I_D-I_0}{\sigma_0\sqrt{2}})\right] \quad \text{---------- (12)}$$

σ_1^2 and σ_0^2 are the corresponding variances of the conditional probability $P(0|1)$ and $P(1|0)$. I_1 and I_0 are bit alignment 1 and 0, I_D threshold bit alignment.

Mostly PIN receivers dominated by thermal noise $(\sigma_T \gg \sigma_S)$ which is independent from average current. Then the BER formed as bellow:

$$BER=\frac{1}{2}erfc(\frac{Q}{\sqrt{2}})=\frac{1}{2}erfc(\frac{\sqrt{SNR}}{2\sqrt{2}}) \quad \text{---------- (13)}$$

In wiretap channel if we have same receiver in legitimate receiver and eavesdropper, it means that both of them have PIN then BER of wiretapper link must be bigger than main link:

$$BER_w>BER_m \quad \text{----------(14)}$$

$$\frac{1}{2}erfc(\frac{\sqrt{SNR_w}}{2\sqrt{2}})>\frac{1}{2}erfc(\frac{\sqrt{SNR_m}}{2\sqrt{2}}) \quad \text{----------(15)}$$

SNR for PIN receivers define as follows:

$$SNR=\frac{I_P^2}{\sigma^2}=\frac{(R_d P_{in})^2}{(4k_BT/R_L)F_n\Delta f+2q(I_p+I_d)\Delta f} \quad \text{------- (16)}$$

In practical issue thermal noise is the dominant element $(\sigma_T \ll \sigma_S)$, thus, we have:

$$SNR_{th-PIN}=\frac{R_L R_d^2 P_{in}^2}{4k_BTF_n\Delta f} \quad \text{----------(17)}$$

Regards to equation (11), we know that:

$$\frac{1}{2}erfc(\frac{\sqrt{SNR_w}}{2\sqrt{2}})>\frac{1}{2}erfc(\frac{\sqrt{SNR_m}}{2\sqrt{2}})$$

Therefore, the error function is a descending function. Subsequently, function parameter in equation we mentioned for BER has opposite behavior then:

$$SNR_w < SNR_m \quad \text{---------(18)}$$

Then we know that for simulating wiretap channel by optical fiber another main rule is that SNR_w is lower than SNR_m .

$$\frac{R_{L_w} R_{d_w}^2 P_m^2}{4k_B T F_n \Delta f} < \frac{R_{L_m} R_{d_m}^2 P_m^2}{4k_B T F_n \Delta f} \quad \text{--------- (19)}$$

In this equation R_L is load resistance in receiver. R_d called responsivity of receiver. F_n is noise factor, T temperature in kelvin, K_B is Boltzmann's constant and Δf is effective noise bandwidth.

PIN receivers have different characteristic with their manufacturer materials. For example, R_d takes different value we show some of them in the figure 6.

Figure 6: Characteristic of PIN.

$$R_{L_w} R_{d_w}^2 \leq R_{L_m} R_{d_m}^2 \quad \text{--------- (20)}$$

From (20), we figure out that by different PIN characteristic we experience different circumstances. By changing Si, Ge, and InGaAs, in two receivers in wiretap channel we have different scenarios.

Same manufacture in wiretap receivers (Bob&Eve)

In this scenario, we consider both wiretapper and legitimate receiver have the same manufacture in their PIN receivers, for example, both have Si in receivers. we sketch the relation between load resistance of the legitimate receiver R_{L_m} and eavesdropper R_{L_w} .

Different manufacture in wiretap receivers (Bob&Eve)

We discuss the same material in the last section. in this part, we want to assess the different material in PIN receivers and check different states that appear.

Figure 7: Same material in wiretap receivers.

We know that each receiver can construct with Si, Ge, InGaAs then we have these states in main a wiretapper as follows:

{Si-Ge}, {Si-InGaAs}, {Ge-Si}, {Ge-InGaAs}, {InGaAs-Si} and {InGaAs-Ge}.

Figure 8: Different material.

Optical fiber wiretap channel with APD

By using an APD receiver we can achieve higher SNR value in constant input power. Therefore, in this section, we want to design a wiretap channel that the legitimate receiver (Bob) has higher SNR value than the wiretapper.

For achieving this goal, we can put an APD optical receiver in the legitimate receiver, while the wiretapper uses a PIN receiver. In

this scenario first, define APD receivers SNR and then by using the equation from the wiretap. We sketch the relation between R_{L_w} and R_{L_m} .

$$SNR = \frac{I_p^2}{\sigma_s^2 + \sigma_T^2} = \quad \text{---------- (21)}$$

$$= \frac{(MR_d P_{in})^2}{2qM^2 F_A (R_d P_{in} + I_d)\Delta f + (4k_B T / R_L) F_n \Delta f}$$

In practical issue thermal noise is dominant element $(\sigma_T \ll \sigma_S)$ If so we,

$$SNR_{th-APD} = \frac{R_L R_d^2 M^2 P_{in}^2}{4k_B T F_n \Delta f} = M^2 SNR_{th-PIN} \text{ ---------- (22)}$$

$$M_{opt} = \left[\frac{4k_B T F_n}{k_A q R_L (R_d P_{in} + I_d)} \right]^{\frac{1}{3}} \quad \text{---------- (23)}$$

In wiretap channel we know that for achieving secrecy capacity we must have:

$$C = \max_{P_x} I(X, Y)$$

It means that we must have maximum SNR in path through legitimate receiver and sender. Therefore, we have:

$$SNR_w < SNR_m$$

With PIN in wiretap receiver and APD in legitimate receiver we have:

$$\frac{R_{L_w} R_{d_w}^2 P_{in}^2}{4k_B T F_n \Delta f} < \frac{R_{L_m} R_{d_m}^2 M^2 P_{in}^2}{4k_B T F_n \Delta f} \quad \text{---------- (24)}$$

Similar to the last section, we demonstrate the relation between the load resistance of the legitimate receiver R_{L_m} and eavesdropper R_{L_w} .

Figure 9: APD characteristic.

Figure 10: Same material, resistance in terms of logarithm.

Figure 11: Different material in terms of logarithm.

Conclusion

In this paper, an optical wiretap channel is proposed to satisfy the secrecy needs between legitimate sender and receiver (Alice and BoB) and to protect transmitted messages from eavesdroppers (Eve). To transmit data securely depending on input and output power, we introduce and evaluate a coefficient between optical link length in the main channel and wiretapper channel in the first section. Additionally, attenuation is also taken into account as a main factor in determining whether the wiretapper channel can be used for message transmission, since it must have a worse situation in terms of attenuation than the main channel. The second step was to simulate wiretap conditions for Bob and Eve using a parameter called attenuation and based on their constructive material, we discussed SNR in receivers (Bob, Eve) of the wiretap channel.

Furthermore, we demonstrated a relationship between resistance load and material type for PIN receivers. As a final step, we used receivers with differing constructive materials (Si, Ge, and InGaAs) to show how resistance loads relate to legitimate receivers and eavesdroppers.

Bibliography

1. D Koenig. "Telegraphs and Telegrams in Revolutionary France". *Scientific Monthly* (1944): 431-437.
2. Historical Sketch of the Electric Telegraph: Including Its Rise and Progress in the United States, GP Putnam, (1852).
3. A C van Heel. "A new method of transporting optical images without aberrations". *Nature* (1954).
4. S Kapany. "Fiber Optics: Principles and Applications". San Diego: Academic Press, (1967).
5. AD Wyner. "The wire-tap channel". *Bell Labs Technical Journal* (1975): 1355-1387.
6. Mahdavifar Hessam and Alexander Vardy. "Achieving the secrecy capacity of wiretap channels using polar codes". *IEEE Transactions on Information Theory* (2011): 6428-6443.
7. Rathi Vishwambhar. "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel". *IEEE International Symposium on information Theory Proceedings (ISIT)* (2011).
8. Csiszár I and Korner J. "Broadcast channels with confidential messages". *IEEE Transactions on Information Theory* (1978): 339-348.
9. G P Agrawal. "Fiber-optic communication systems". John Wiley and Sons, (2012).
10. J Hecht. "The "Lost Generation of Fiber Optics". Optics and Photonics News, (1999).
11. Hansell Clarence W. "Picture transmission". U.S. Patent No. 1,751,584 (1930).
12. H Lamm. "Flexible Optical Instrument". Z. Instrumentenk (1930): 579-581.
13. van Heel and Abraham CS. "A new method of transporting optical images without aberrations". *Nature* (1954): 173.
14. Potter Robert J and Cecelia E Beasor. "The history and evolution of fiber optics". *International Society for Optics and Photonics* (1968): 14.
15. Endo Hiroyuki., *et al*. "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels". *IEEE Photonics Journal* (2015): 1-18.
16. Sun Xiaole and Ivan B Djordjevic. "Physical-layer security in orbital angular momentum multiplexing free-space optical communications". *IEEE Photonics Journal* (2016): 1-10.
17. Laourine Amine and Aaron B Wagner. "The degraded Poisson wiretap channel". *IEEE Transactions on Information Theory* (2012): 7073-7085.
18. Guan Kyle., *et al*. "Physical layer security in space-division multiplexed fiber optic communications". in In Signals, Systems and Computers (ASILOMAR), 2012 Conference Record of the Forty Sixth Asilomar Conference (2012).
19. Zyczkowski M., *et al*. "Optical fiber sensors as the primary element in the protection of critical infrastructure especially in optoelectronic transmission lines". *Safety and Security Engineering* (2013).
20. Guan K., *et al*. "Physical layer security in space-division multiplexed fiber optic communications". In Signals, Systems and Computers (ASILOMAR) (2012).
21. Lonnstrom Andrew., *et al*. "Robust secure goodput for massive MIMO and optical fiber wiretap channels". in Signal Processing Advances in Wireless Communications (SPAWC), IEEE 18th International Workshop (2017).
22. M Soltani and Z Rezki. "Optical Wiretap Channel with Input-Dependent". in International Zurich Seminar on Information and Communication (IZS) (2018).
23. Mohammad Reza Deylam Salehi and Hassan Tavakoli. "Achieving Secure Communication over Wiretap Channels Using the Error Exponent of the Polar Code". *Engineering Letters* 30.1 (2022).