IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 1, Ser. III (Jan. –Feb. 2022), PP 01-05
www.iosrjournals.org

Enhance Data Security Method using Partially Transmitted Sequences and Fast Fourier Transform

Mamta Pant[1], Arundhati Waliya[2]
[1] *HR Institute of Technology, Uttar Pradesh, India*
[2]*Associate Professor, Dept. of Computer science Engineering, HR Institute of Technology, Uttar Pradesh, India*

Abstract - *Data security is very crucial in today's digital world, protecting a digital data from unwanted action of unauthorized users like cyber-attack. Using some advanced technologies we can try to protect over data in a variety of ways. In this research work we proposed technique of partially transmitted sequences along with the fast Fourier transform for physical layer security. The performance of the proposed technology is based on the complementary cumulative distribution function of low crest which enhance the level of security.*

***Key Words*:** *Crest Factor, Fast Fourier Transform, Partially Transmitted Sequences*

Date of Submission: 06-02-2022 Date of Acceptance: 19-02-2022

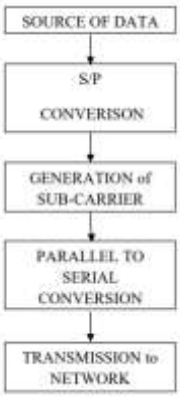
I. Introduction

The world has largely become data driven and henceforth protection of data has become paramount. Many a times the encrypted data is vulnerable to third party attacks. As the internet usage has become indispensable in this digital age, almost all kinds of data is shared and stored online. So it is essential to protect and safeguard our data from intruders and attackers at all costs. The general encryption algorithms work from the application layer of the OSI model. So safeguarding the system from the physical layer is necessary for bit level security. Tampering the data from the physical layer of OSI is very difficult and non-feasible. The crest factor of the system is the performance metric used to gauge the system performance.

Cyber security is method to protect your computer system, mobile device, electronic system and data and networks from malicious attack like theft, disclose or damage from hackers. In today's world we are totally dependent on internet and other wireless networks like Wi-Fi or Bluetooth which is the easy for hackers to access your device without your information that's why cyber security is very important in contemporary world.

1.1 Data Physical Architecture

The transmission and functionality of the user data is easily understood by the following illustrative diagram:



It shows the origin of the data from data source to towards transmission. In the transmission process the data originates from the data source. Then it gets into the serial to parallel converter. Next follows is the generation of the sub carrier. The data is transmitted through the sub carrier signal. Then in the consecutive step the signal is processed for parallel to serial conversion. Finally after all these processes, the signal is transmitted to the network. The optical networks use a very large portion of the available bandwidth. The structure followed for the transmission of the signal is always of the serial nature. Hence the serial to parallel and parallel to serial conversions are carried out as a part of the transmission processes. A similar process also applies at the receiving end. An exactly opposite process of transmission method is applied for reception purpose. The signal that is to be transmitted and received has to abide by these conversion techniques in order to be correctly sent and received.

1.2 The Significance of Crest Factor

The crest factor of the system designed is explained as the ratio of the peak power to that of the average power of the system.

$$CrestFactor(CF) = \frac{\text{maximum } \{Z(t)^2\}}{mean\ \{Z(t)^2\}}$$

Z (t) denotes the transmitted signal Maximum represents the peak of the signal Mean represents the average value of the signal the importance of the CF is attributed to the fact that the CF signifies the amount of signal deviation from the mean power which makes it more susceptible to third party attacks.

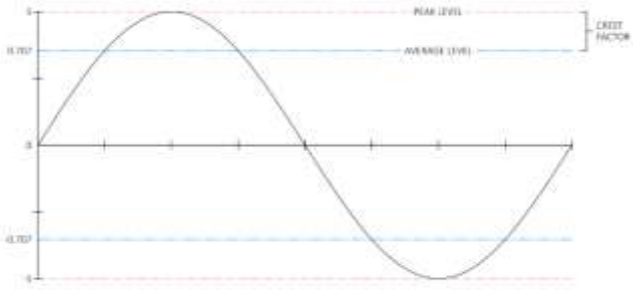


Fig -1: Crest factor of a sine wave

II. Problem Formulation

The main objective of this proposed work is to lessen the Crest Factor of the system. This would infer minimum deviation of the signal from the average power. This ensures that the abrupt signal peaks would not be there in the system and hence it would not be recognizable. This would reduce the perceptibility factor and the data would be difficult to be identified by the intruders. As the data protection and confidentiality is a major area of concern, it is essential to use minimum crest factor. But selection of crest factor is to be done prudently such that it doesn't make the system complex because data integrity must be maintained at all measures.

III. Techniques to reduce crest Factor

There are some technology available which can be used to reduce the crest factor and have their merits and demerits.

Clipping and filtering - Clipping is the one of the conventional method to reduce crest factor, in which clipping can caused sharp corner in input signal which lead to reduce unwanted out of band emission.

Tone Rejection - In the technique of tone rejection, it is identified as which of the frequencies are causing a surge in the crest factor of the system. They are identified and summarily rejected as carriers for user data thereby reducing the crest factor.

Partially Transmitted Sequences - The concept of the partially transmitted sequences lies in the fact that the technique tries to leverage the variations in the signal crest factor as there are shift vectors added to it in the form of complex numbers.

IV. Mathematical Modeling of Partially Transmitted Sequences

Consider the sample space of the shift vectors are given by:

$$S\_B = \begin{matrix} b1 \\ b2 \\ \vdots \\ \vdots \\ bn \end{matrix}$$

Simultaneous versions of the data are generated given by:

$$Y = \begin{matrix} Y1 \\ Y2 \\ \vdots \\ \vdots \\ Yn \end{matrix}$$

The exhaustive search tries to find out:

□□□□□□□ = (□□□(□□1,□□2,□□3, … … . □□□))

The shift that results in the crest factor to fall to the minimum value is used for the final data transmission. The PSD of such a shifted version of the data is given mathematically as:

$$\sum_{n=0}^{K-1} \frac{\lambda_n(\hat{H}(f)-\hat{H}_n(f))}{(\lambda_n\hat{H}(f)-\hat{G}_n(f))^2} = 0$$

G represents the shift vector sample space, 𝑃(𝑓) is the PSD And 𝑃𝑃 (𝑓) is the statistical average of (𝑓).
The variation in the maxima of the modulated envelope of H (f) is given by:
𝑃𝑃 (𝑓) = 1(1 −). 𝑓. 2, 𝑓 = 0, 1,… … … …. 𝑓 − 1
The PSD after vector shifts is computed as:

$$\hat{H}^{k+1}(f) = \left[\sum_{n=0}^{N-1} \frac{\mu_n \hat{H}_n^{(k)}(f)}{\left(\mu_n \hat{H}_n^{(k)}(f)+\mu_n \hat{H}_n(f)\right)^2}\right] + \left[\sum_{n=0}^{N-1} \frac{\mu_n \hat{H}_n^{(k)}(f)}{\left(\mu_n \hat{H}^{(k)}(f)+\hat{H}_n(f)\right)^2}\right]^{-1}$$

Here, f represents the frequency domain dependence, B stands for the shift vector's sample space in the magnitude-square form, we get

$$Z(f) = 2\sum_{n=0}^{N-1} |h_n(f)|^2$$

Z (f) denotes the f-domain total magnitude; hn denotes the samples in discrete frequency
The subsequent process is the rigorous search for the shift causing the signal to attain the minimal values of CF:

$$Sh(f) = \begin{bmatrix} s_0^{(0)}Y_0^{(0)} & s_1^{(0)}Y_1^{(0)} & \cdots & s_{N-1}^{(0)}Y_{N-1}^{(0)} \\ s_0^{(1)}Y & s_1^{(1)}Y_1^{(1)} & \cdots & s_{N-1}^{(1)}Y_{N-1}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ s_0^{(k-1)}Y_0^{(k-1)} & s_1^{(k-1)}Y_1^{(k-1)} & \cdots & s_{N-1}^{(k-1)}Y_{N-1}^{(k-1)} \end{bmatrix}$$

The possibility of finding a vector leading to decreased CF is given by
b€min (𝑃𝑓)
The Hermitan transpose is given by b, the kth value order is denoted by 𝑓. 𝑓. (𝑓)
The change or variation in the instantaneous value from the mean is given by

$$V(f) = \sum_{k=0}^{k-1} s.d._k\, u_n b_n^i$$

s.d. is the standard deviation , (𝑓) is the probability distribution vector, 𝑃𝑓 (𝑓) is a shift combination vector, Computing the Eigen values, we get

$$A(f)A^i(f) = \sum_{p=0}^{p-1} \sigma_p^2(f) u_p(f) v_n^i(f)$$

Here, 𝑃𝑓 2 (𝑓) is the mth Eigen value of the Eigen decomposition.
The frequency dependence is therefore given by:

$$H(f)H^i(f) = \sum_{k=0}^{k-1} s.d._k^2(f) u_n(f) u_k^i f)$$

The Eigen values extend to… N-1 is all zero.
The CF exhibits a probabilistic swing of:

$$s.d._n^2(f) = \sum_{k=0}^{k-1} |u_{k=1}^n(f)|^2 \left|Y_{k=1}^{k=n}(f)\right|^2$$

𝑓. 𝑓.𝑓 2 (𝑓) depicts the variance or swing in terms of probability
Putting |𝑃𝑓=1 𝑃𝑓=𝑓 (𝑓)| 2 = µ(𝑓) & operating 𝑓. 𝑓.𝑓 2 (𝑓) / ∑ µ𝑓 (𝑓) (𝑓) 𝑓=𝑓−1 𝑓=0 , the following is obtained:

$$\hat{H}^{(n)}(f) = \frac{\sum_{k=n=0}^{p-1} \mu_k^{(n)}(f)\left|Y_{k=0}^{k=n-1}(f)\right|^2}{\sum_{k=0}^{k=n-1} \mu_p^{(n)}(f)}$$

Here, 𝑃(𝑓) (𝑓) represent the discrete f-based samples of H
n denotes the sample number
n=0,1,2……,k-1
Considering a total sample space of B vectors,,

$$\int_{-\infty}^{\infty} B(t,f)df = |y(t)|^2$$

(𝑓, 𝑓) represents the dependence of B on (t,f), Hence we get

$$|y(t)| = \int_{-1/2}^{1/2} \exp(j2\pi ut)\, dY_x(u)$$

(𝑓) is the equi-probable df between +1/2 & -1/2

V. Results

The system is designed on the programming and simulation tool MATLAB (Matrix Laboratory) to facilitate the mathematical operations performed on data streams. The PTS is applied and hence after, the windowing functions are applied in the peak window. The results obtained with the different peak windows are shown in the subsequent section.

1. Gaussian Windowing –

The Gaussian Function, is mathematically defined as-

$$w(x) = e^{\frac{-1}{2}\left(\mu\frac{x}{\frac{N}{2}}\right)^2} \qquad 0 \le |x| \le \frac{N}{2}$$

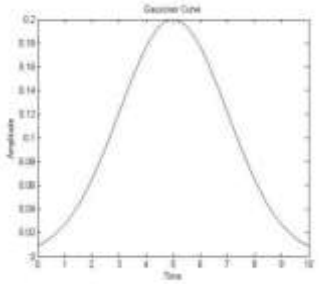


Fig -2: Gaussian Curve

It is important to note that the windowing function rises in such a manner that the maximum value is less than unity and does not have a constant increasing or decreasing gradient. Hence it reduces the peaks more than the adjacent values thereby reducing the CF.

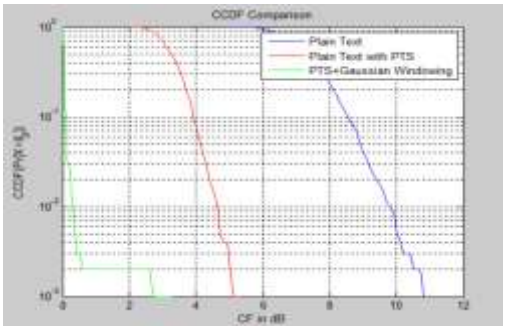


Fig -3: Proposed Techniques with Gaussian Peak Windowing

The CCDF above exhibits the variation of the CF with respect to the threshold in CF. The comparison has been made among 3 systems viz. Plain Text, Plain Text with PTS, and Plain Text with PTS + Gaussian Windowing. It can be clearly seen that the proposed technique of PTS + Gaussian Windowing outperforms the other two techniques thereby clearly indicating that the proposed system achieves better CF reduction.

VI. Conclusion

It can be concluded from previous discussions that many a times the encrypted data is vulnerable to attacks. As the internet usage has become indispensable in this digital age, almost all kinds of data is shared and stored online. So it is essential to protect and safeguard our data from intruders and attackers at all costs. The general encryption algorithms work from the application layer of the OSI model. So safeguarding the system from the physical layer is necessary for bit level security. Tampering the data from the physical layer of OSI is very difficult and non-feasible. Hence physical layer security is mandatory which is also called bit let security. The proposed technique is able to achieve low crest factor value by using the PTS algorithm the essence of which lies in the fact that the partially transmitted sequences lies in the fact that the technique tries to leverage the variations in the signal crest factor as there are shift vectors added to it in the form of complex numbers. The shift vectors result in the modification of the time domain behavior of the signal or the data stream. The crest factor changes with the addition of the vectors in the sample set each of the vector additions result in a different value of the crest factor and hence causes the CF to change. In the PTS technique, the shift vector b which causes the minimal crest factor value is searched among all the version of the signal X. The flip side to the PTS scheme is the fact that the exhaustive search of the PTS increases the complexity of the system manifold. Hence, keeping in mind the system requirements the

PTS technique is to be designed else I would lead to infeasibility in system implementation. Moreover, he PTS is effective in reducing the CF but has some associated challenges such as: as the sample space of shifts increases, the complexity of search increases, residual peaks may exist even after PTS is applied, there is NO limit or limit rule to as how many shifts sample tests will results in reduction of CF to the desired value, Sub-blocking increases the chances of CF reduction by increases the complexity of the system. Hence it is necessary to use some additional feature with PTS to reduce the CF below a particular threshold. This is done using the residual crest detection and applying a windowing function to decrease the residual crests. A comparative analysis shows that the performance of the proposed system is better compared to previous work. The evaluation parameter has been chosen to the CCDF of Crest Factor (CF).

References

[1]. Zhiyi Wang ,Jun Cao ,Rui Deng ,Yi Liu,Jing " Time-frequency domain encryption with SLM scheme for physical-layer security in an USER DATA system", IEEE 2018
[2]. Amber Sultan ,Xuelin Yang , Adnan A. E. Hajomer ,Weisheng Hu," Chaotic Constellation Mapping for Physical-Layer Data Encryption in USER DATA", IEEE 2018
[3]. Adnan A. E. Hajomer , Xuelin Yang ,Weisheng Hu, "Chaotic Walsh–Hadamard Transform for Physical Layer Security in USER DATA", IEEE 2017
[4]. HM Furqan, JM Hamamreh , "Enhancing physical layer security of OFDM systems using channel shortening", IEEE 2017
[5]. W Liu, M Li, G Ti, X Tian, Q Liu "Transmit filter and artificial noise aided physical layer security for OFDM systems",IEEE 2016
[6]. G Shiqi, X Chengwen, F Zesong," Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper", IEEE 2016
[7]. Y Zou, J Zhu, X Wang, VCM Leung," Improving physical-layer security in wireless communications using diversity techniques",IEEE 2015
[8]. E Jorswieck, S Tomasin, A Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing",IEEE 2015
[9]. A Muk., S. Fakoorian, J Huang," Principles of physical layer security in multiuser wireless networks: A survey", IEEE 2014
[10]. ZE Ankaral, M Karabacak," Cyclic feature concealing CP selection for physical layer security", IEEE 2014