IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Data Security using Partially Transmitted Sequences and Fast Fourier Transform

Prateek Kumar Dohare[1*], Preeti Ahirwar[2]

[1,2]Dept. of Computer Science, Vikrant Institute of Technology & Management, Indore, India

[*]*Corresponding Author: dohare.prateek0@gmail.com, Mob.: +919039723757*

Available online at: www.ijcseonline.org

Accepted: 18/Nov/2018, Published: 30/Nov/2018

Abstract— Data security can be achieved in a variety of ways. Often encryption algorithms are prone to attacks and hence can't ensure high data security for classified and highly confidential data, the reason being the fact that encrypted data is often perceptible and hence more prone to attacks due to its existence on the application layer level of the OSI model. Hence the necessity for physical layer security arises. The proposed technique uses partially transmitted sequences along with the fast Fourier transform for physical layer security. The performance of the proposed system is based on the complementary cumulative distribution function (CCDF) of the crest factor of the data. It has been shown that the proposed system attains a low crest factor therefore reducing the perceptibility and increasing the level of security.

Keywords— Complementary Cumulative Distribution Function (CCDF), Crest Factor (CF), Fast Fourier Transform (FFT), Partially Transmitted Sequences (PTS), Peak to Average Power Ratio (PAPR).

I. INTRODUCTION

Most of the data transmissions these days are migrating towards wireless data transfer due to the following reasons:

1) Lower Cost
2) Ease of maintenance
3) Mobility
4) Scalability

However due to the unguided media of transmission between the sender and receiver, chances of attacks increase manifold compared to wired or guided media.[1]-[3] It is customary to use encryption algorithms but they do not guarantee security owing to the fact that encrypted data is often highly perceptible and hence attract more attacks. Guided media also encounters the same challenges, mostly at the routing joints. Hence, the design of physical layer security mechanisms is mandatory as the most critical aspect is making the system immune against attacks. One of the most effective ways to do the same is by maintaining a noise like low power profile for the transmitted signal. However, this is the most difficult challenge in data transmission since it exhibits sudden surges or peaks in signal power that makes it detectable to possible attackers. [6] Hence it becomes mandatory to reduce such peaks to decrease perceptibility. The performance metric that measures the surges in power is called the crest factor. The objective of the system design would be reduction in the crest factor of the system. This would lead to lesser deviation from average power of the system in terms of the fact that the sudden surges in the power would be absent from the system. This would lead to lesser perceptibility of the transmitted data by possible adversaries. This is a measure by which the threats can be thwarted from possible attacks. However the choice of an appropriate system for crest factor reduction is to be chosen so that the side information does not yield excessive complexity to the system.[5] The basic nature of such a system would be keeping the original data intact.

The rest of the paper is organized as follows: Section II describes data crest factor (CF), Section III presents the partially transmitted sequence (PTS) algorithm, and Section IV describes the modified PTS algorithm, Section V shows the resultant image, and finally Section VI concludes the research work.

II. THE DATA CREST FACTOR (CF)

The crest factor decides the chances of perceptibility of the data. Often the crest factor is measured in terms of the deviation of the data signal above a particular threshold. The signal lying below a particular threshold can be visualized as the chances to produce erroneous reception. Let the threshold be given by K.[4]

The probability that the strength will lie below the threshold is given by:

$$\Pr[mod\{x(t)] < T \quad (1)$$

Here,
Pr represents probability
X(t) is the time domain OFDM-PON signal
T is the threshold
The occasion when the signal strength dips below the prescribed threshold is called the fading dip of the system. The visualization of such a dip occurring in transmission is given by:

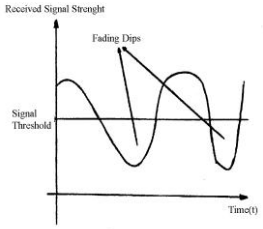

Figure 1. Chances of Fading Dips

The threshold (T) is used to decide the fading dip. The threshold value may vary system to system.

The fading dips result in the increased chances of bit errors in the reception. Thus is to be ensured that the fading dips are avoided. This clearly indicates the fact that clipping the signal to reduce the crest factor of the system is not an effective measure to ensure security for the system. [7]-[8] This paves the path for the need of different crest factor reduction techniques that would not adversely affect the error rate of the system. However, the chances for the system to attain a crest factor greater than a particular value of threshold crest factor are given by the complementary cumulative distribution function (CCDF) of the system.
The CCDF of a particular random variable X is defined as:

$$Y=\Pr[X > X_0] \quad (2)$$

Here,
Y is the CCDF value
X is random variable denoting the PAPR
X0 is the instantaneous PAPR
Pr stands for probability.
Often CCDF is represented as:

$$CCDF = 1 - CDF \quad (3)$$

Here,
CCDF represents the complementary cumulative distribution function
CD represents the cumulative distribution function
A steeper fall in the CCDF depicts a lesser crest factor value. The CCDF probabilistic approach is needed as the data generated as the plain text can be random hence the final signal would be random. Hence a non-deterministic stochastic approach using the CCDF suits the purpose.
The problem with data security lies in the fact that the high swing in the strength of the signal is responsible for increased perceptibility of the data transmission. In this section we evaluate the reasons for the increased crest factor for the designed systems:
Let the time domain signal for the signal be given by;

$$X_i(f) = \sum_{n=0}^{N-1} x(n) v_n^{(i)} \exp(-j2\pi fn) \quad (4)$$

Where,
i=0, 1, 2,……,(n-1)
n are the number of sub carriers
X(f) is the frequency spaced signal
Let the number of users be N
Let the bandwidth requirement of each user be W. The complex exponential is needed for a real time transmission of the signal through wireless media.
Then the overall bandwidth available to the system can be given by:

$$C_0 = NW \quad (5)$$

N is the number of multiplexed data streams through the channel. The rate of sampling the signal should be twice or equal to the maximum bandwidth and according to Shannon's sampling theorem:

$$I \leq [2NW] \quad (6)$$

Here,
I represents the aliasing factor.
The CDF of the above function can be represented by λ_0 and is given by:

$$1 - \lambda_0 \approx 4\pi\sqrt{C_o}\exp(-2\pi C_o) \quad (7)$$

Here,
C_0 denotes the overall bandwidth of the system
The overall power spectral density (psd) of the system can be given by:

$$\hat{S}(f) = \frac{\sum_{n=0}^{n-1} \lambda_n |X_n(f)|^2}{\sum_{n=0}^{n-1} \lambda_n} \quad (8)$$

Here,
$\hat{S}(f)$ represents the PSD
X_N represents the sampled version of the signal X with n samples.
The PSD the spectral coverage of the data stream.

III. THE PARTIALLY TRANSMITTED SEQUENCES (PTS) ALGORITHM

The technique exploits the fact that the time domain signal is highly sensitive to phase shifts. It can be intuitively inferred that phase shifts would lead to the change in the way the N sinusoids superimpose on each other thereby changing the nature of the time domain transmitted signal. Addition of certain phases would lead to the decrease in the peak values whereas addition of certain other phases would increase the peak value of the signal. Thus phases are added (generally equidistantly) to modify the peak value. The results can be further improved if the degree of freedom (DoF) [6] for phase addition could be increased.

This is exactly what is done in the partially transmitted sequences technique. The parallel data stream coming from the serial to parallel converter is portioned into disjoint sub blocks. This increases the degree of freedom for phase additions to the sub blocks and increases the probability of further reduction in the peak value and subsequently the crest factor (CF) value. After different phases are added, an exhaustive search is carried out in the optimizer block to select the phase that results in minimum CF. It should be noted though that such an optimization problem substantially increases the complexity of the system, [8] though it does not remain a hindrance in practically using PTS since advancements in system on chip technology has made it possible to implement complex algorithms on ICs. Although PTS exhibits considerable CF reduction capability, yet the search for more efficient algorithms possessing higher reduction competence remains an active area of research because the exhaustive search for the optimal phase and optimal partitioning of the data stream increases the system complexity considerably.[5]

From the previous discussions, it can be concluded that the partially transmitted sequences (PTS) is one of the most effective techniques for the reduction of crest factor and hence can be used to enhance the physical layer security of encrypted data at the physical layer level encryption mechanism which yields higher security compared to application layer security mechanisms. The block diagram of the PTS algorithm has been shown in the figure below:

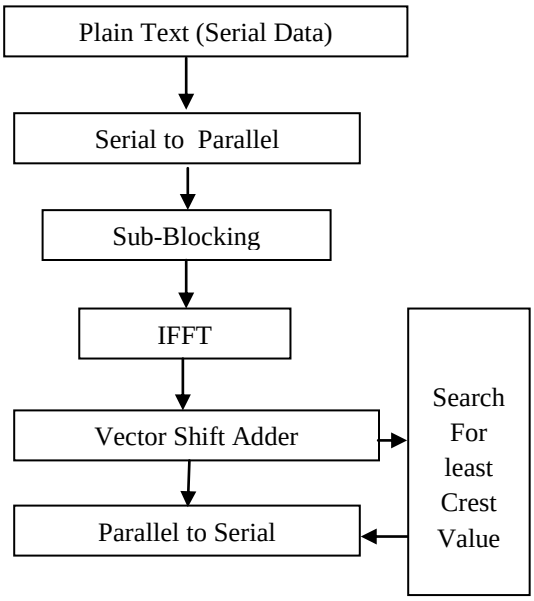

Figure 2. Block Diagrammatic Implementation of PTS Algorithm

The use of the Fourier Transform gives complex values thereby making the data less perceptible compared to simpler mappings and real transforms.

The mathematical formulation here in the IFFT block for the implementation of the Fourier Transform is given by:

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j\omega t} dt$$

Here,

X(f) represents the data stream after the Fourier Transform

X(t) is the data stream prior to application of Fourier Transform

ω represents the kernel vector

The Fast Fourier Transform is a faster way to implement the conventional Fourier Transform.

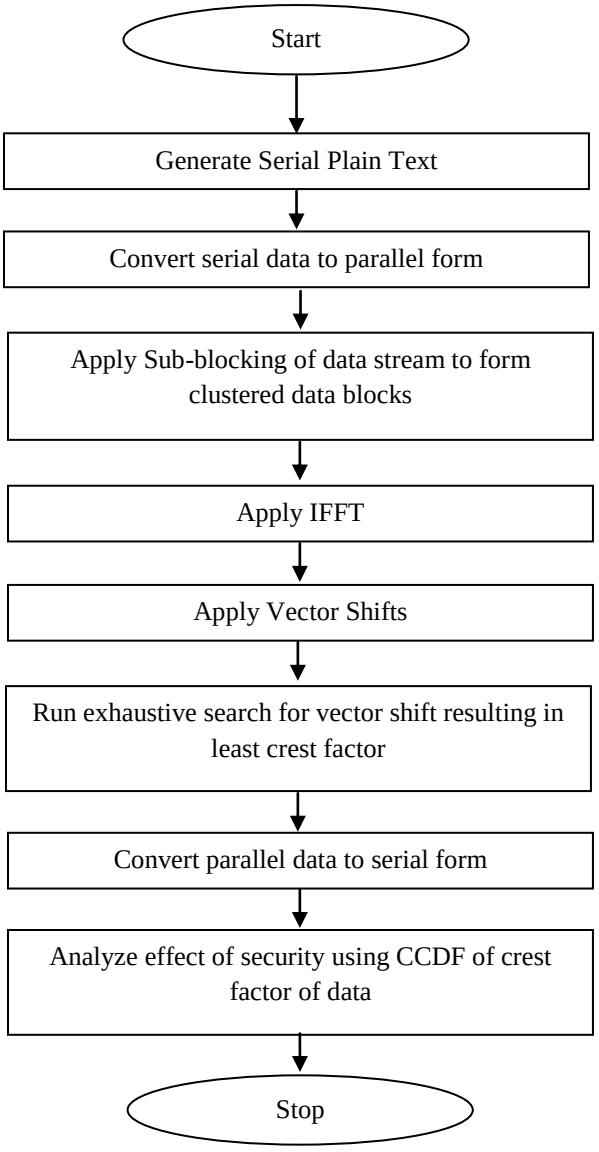

Figure 3. Flowchart of Proposed Algorithm

IV. THE MODIFIED PTS ALGORITHM

The PTS can be modified to remove residual peaks existent from the application of the PTS technique. This needs the concept of peak windowing. Peak windowing is a technique of detecting and removing residual peaks. This can be done using weighted functions.

The proposed system can be explained using the following algorithm:

Step1. Generate random binary plain text.

Step2. Detect its residual crests after PTS using threshold.

Step3. Obtain the locations of the crests and adjacent samples to decide the peak window.

Step4. Design a peak windowing function to fit in the crest window.

Step5. Multiply corresponding values of the signal and the windowing function.

Step6. Plot the CCDF of the CF of the obtained signal.

Step7. Compare the results with conventional PTS technique and previous work.

The Windowing Functions designed in this case is the inverse Gaussian function defined as:

The inverse Gaussian Function, which can be mathematically expressed as;

$$w(n) = -e^{\frac{-1}{2}\left(\alpha\frac{n}{\frac{N}{2}}\right)^2} \quad 0 \le |n| \le \frac{N}{2} \qquad (9)$$

Then the windowing function is multiplied with the signal after application of PTS in the peak window period, which can be mathematically expressed as;

$$C(n) = x(n).w(n) \qquad (10)$$

Where, x(n) is the original data signal after application of PTS and w(n) is the winnowing function.

V. RESULTS

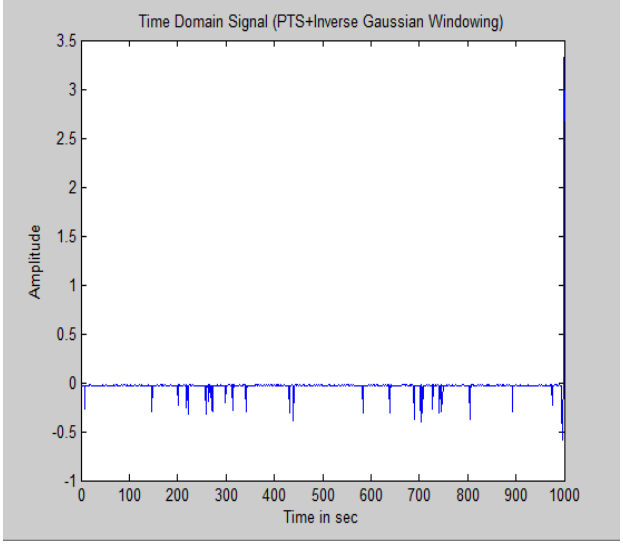

Figure 4. Residual Crests

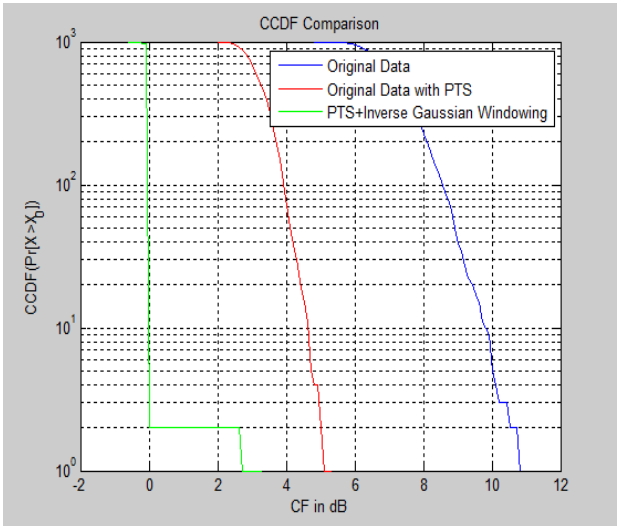

Figure 5. Comparative CCDF Analysis

The analysis of the results can be carried out using the CCDF values of CF for the proposed and the existing system. The following table tabulates the required values. It can be seen that the proposed system attains better crest factor (CF) reduction compared to both PTS and previous work.[1]

Table 1. Comparative CCDF Values for X_0

S. No	Technique	Probability	X_0
1.	Original Data	10^{-3}	10.7dB
2.	Original Data with PTS	10^{-3}	5.2dB
3.	PTS + Inverse Gaussian Windowing	10^{-3}	2.6dB
4.	Base Paper (Adnan A.E. Hajomer et al.) [1]	10^{-3}	8.7dB

VI. CONCLUSION

It can be clearly seen from the CCDF curves as well as the tabulation of CCDF that the proposed system attains better results compared to conventional PTS. It is worth mentioning here that though the PAPR reduction capability of PTS increases with the increase in the size of the phase vector added and also the level of partitioning of the data blocks, it increases the system complexity

substantially. In the proposed approach, we have put forth an approach which tries to detect the neighborhood of the residual peaks of the data signal after PTS has been applied and subsequently apply peak windowing. It should be noted though that the design of the windowing function is critical as extension of the windowing function beyond the peak window is bound to affect the signal sample where peaks do not appear thereby degrading the performance of the system. It can be concluded from the results that an appropriate mathematical windowing function in the peak window period can achieve much better CF reduction compared to the conventional PTS algorithm without enhancing the system complexity. This ensures high level of security without increasing system complexity above bounds. A comparative analysis shows that the proposed system attains better crest factor reduction compared to latest existing techniques.

REFERENCES

[1]. Adnan A. E. Hajomer, Xuelin Yang, Weisheng Hu, "Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform", IEEE 2017

[2]. Chongfu Zhang, Wei Zhang, Xiujun He, Chen Chen, Huijuan Zhang, Kun Qiu,, "Physically Secured Optical OFDM-PON by Employing Chaotic Pseudorandom RF Subcarriers", IEEE 2017

[3]. Wei Zhang, Chongfu Zhang, Chen Chen, Wei Jin, Kun Qiu, "Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON",IEEE 2016

[4]. Wei Zhang ,Chongfu Zhang, Wei Jin, Kun Qiu, Chen Chen, " Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in OFDM-PON systems", IEEE 2016

[5]. Xiaonan Hu, Xuelin Yang, Zanwei Shen ,Hao He, Weisheng Hu ,Chenglin Bai, " Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON",IEEE 2015

[6]. Xuelin Yang, Xiaonan Hu ,Zanwei Shen, Hao He, Weisheng Hu, Chenglin Bai, "Chaotic signal scrambling for physical layer security in OFDM-PON",IEEE 2015

[7]. Bo Liu, Lijia Zhang, Xiangjun Xin, Yongjun Wang, "Physical Layer Security in OFDM-PON Based on Dimension-Transformed Chaotic Permutation", IEEE 2014

[8]. Wei Zhang , Chongfu Zhang, Wei Jin, Chen Chen, Ning Jiang, Kun Qiu, "Chaos Coding-Based QAM IQ-Encryption for Improved Security in OFDMA-PON", IEEE 2014

