[1]Navashish Kaur

[2]Dr. Dinesh Kumar

A Review and Analysis of Existing Approaches for Imperceptibility Based Proactive Security Measures for Wireless Networks

Journal of Electrical Systems

Abstract: - A lot of security systems rely on devising mechanisms which rely on detecting security threats or possible attacks. Such security mechanisms are typically terms as intrusion detection systems (IDS). When such as system is deployed at the network layer, it is termed as a network intrusion detection system (NIDS). While ID or NIDS is typically a rule based reactive security mechanism, with emergence of AI and Quantum computing, reliance on conventional IDS or encryption mechanisms lead to high possibility of successful security attacks. Hence, research is focussing on proactive approaches which can render imperceptibility to data transmission in a network. In the proposed work, a crest factor reduction mechanism based on the selective mapping (SLM) approach which renders the property of chaos to the system. The SLM technique multiples the plain text with complex vectors whose pattern is known only to the sending and receiving end, and produces relatively high security, through implementation of chaos. The analysis of the crest factor needs to be evaluated in terms of the complementary cumulative distribution function (CCDF) of the crest factor. It is shown that the proposed approach attains lower PAPR compared to existing approaches in the domain.

Keywords: Wireless Network Security, Crest Factor, Data Imperceptibility, Selective Mapping, Phase Vector, complementary cumulative distribution function (CCDF)

I. INRRODUCTION

With emerging technologies such as internet of things (IoT) and fog computing, there has been a rapid shift towards wireless networks. However, owing to the wireless nature of data transfer, security happens to be one of the major concerns of wireless networks [1]. Needless to say, the security of data is of enormous importance today. The world has predominantly become data-driven, making data protection essential. Encrypted data is frequently susceptible to third-party assaults [2]. In this digital era, internet usage has become essential, resulting in the widespread sharing and storage of various types of data online. It is imperative to protect and secure our data from intruders and attackers at all costs. General encryption techniques operate at the application layer of the OSI model which may get compromised due to emerging approaches such as quantum machine learning whose brute force power exceeds the chaos generated through conventional security mechanisms [3]. Delving into the deeper layers of the OSI model and applying bit level encryption happens to be the safest form of security. As data processing capabilities on hardware platforms are becoming more advanced with the passage of time, hence cryptanalysis is also becoming more sophisticated. Therefore, complete reliance on encryption mechanisms stand the chances of compromise on security especially for wireless networks [4]

This has led to the search for mechanisms to make wireless data transfer as imperceptible as possible. In this context, a fundamental metric is the crest factor or the peak to average power ratio. It is the ratio of the peak to average power of the transmitted data stream [5]. Lower values of the crest factor would result in lesser spikes in the power and in turn would make the data transmission through wireless media less perceptible. One way to measure how well a system is doing is by looking at its crest factor. Proactive network-level security denotes the tactics and technologies employed to foresee and avert threats prior to their exploitation of weaknesses within a network [6]. An essential factor in enhancing network security is the optimization of signal transmission, which can be affected by Peak-to-Average Power Ratio (PAPR). Elevated PAPR in wireless communication systems results in transmission inefficiencies, increasing vulnerability to assaults and diminishing overall performance. Integrating PAPR reduction techniques into network security protocols can boost signal transmission efficiency, providing an extra layer of security. The peak to average power ratio is defined as [7]:

[1] Department of Computer Science and Engineering1,2
GZSCCET, MRSPTU Bathinda, Punjab, India1,2
Corresponding Author: Navashish Kaur, navashish@gmail.com

$$CF\ or\ PAPR = \frac{Peak\ Power\ \{x(t)\}}{Average\ Power\ \{x(t)\}} \quad (1)$$

The model for the wireless data transmission model is depicted in figure 1

.

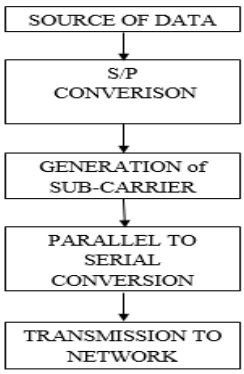

Fig.1 The data transfer mechanism in wireless networks

Data comes from somewhere throughout the wireless medium through several sources or IoTDs. The next step is for it to enter the parallel to serial converter. The creation of the sub carrier comes next. The sub carrier signal is used for data transmission [8]. The following step involves processing the signal for serial to parallel conversion. At last, the signal is sent to the network following all these procedures. Out of all the bandwidth that is available, optical networks consume the most [9].

In every case, a serial structure is used for the signal transmission. Translations from serial to parallel and vice versa are thus performed during transmission [10]. On the other side, the procedure is very much the same. The challenging aspect with the multi user data transmission in wide area network systems is the fact that the increased perceptibility of the data signal allows the adversaries to detect is more easily and attack them. This makes it necessary to make the data transmission imperceptible thereby rendering security to the data transfer [11].

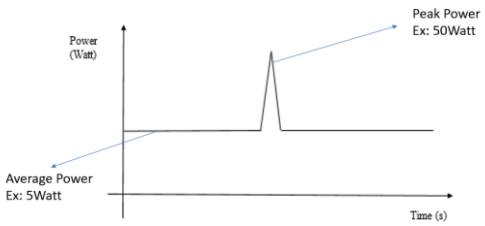

Fig. 2 Concept of PAPR

Figure 2 depicts the concept of the PAPR of the system defined by equation 1. However, reducing the PAPR has its associated challenges. Some of the common techniques for reduction of PAPR are presented in the subsequent section [12].

II. LITERATURE REVIEW ON EXISTING METHODS

Different techniques can be used to reduce the crest factor and have their own merits and de-merits. The most popular ones are described in the subsequent section.

Clipping

Clipping is the technique in which a threshold is chosen and the part of the signal above it is clipped resulting in reduces crests [13].

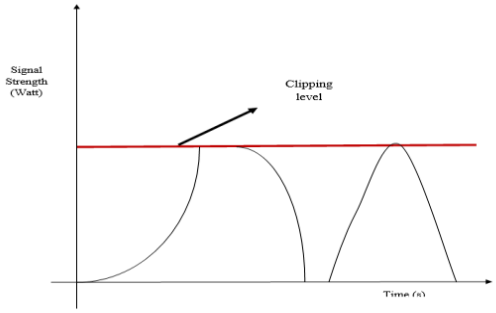

Fig. 3 Clipping Process

Figure 3 depicts the clipping process, for the strength beyond the threshold.

Tone Injection

By employing the tome rejection method, we may determine which frequencies are responsible for the system's crest factor surge. By eliminating them as potential data carriers for users, we lower the crest factor [14].

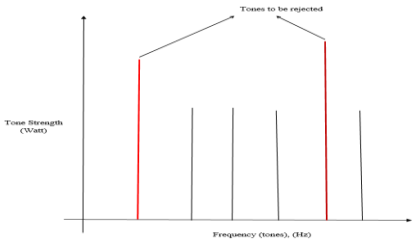

Fig.4 Tone injection

Figure 3 depicts the tome injection process for the data carriers in the frequency domain.

Selective Mapping (SLM)

The selective mapping (SLM) technique aims to exploit differences in the signal crest factor by using shift vectors represented as complex values [15].

The shift vectors alter the temporal characteristics of the signal or data stream. The crest factor varies with the incorporation of the vectors in the sample set. (b1, b2……bn). Each vector addition yields a distinct crest factor, hence altering the PAPR. In the SLM approach, the shift vector b that minimizes the crest factor value is identified among all versions of the signal X [16]. The selective mapping relies on reduction of the PAPR based on different phasor products. Integrating PAPR reduction strategies inside network-level security frameworks might operate as a preemptive approach to mitigate security vulnerabilities. Reducing PAPR decreases power consumption, mitigates the likelihood of signal distortion, and enhances the network's resilience against external interference, including jamming or interception. Consequently, communication systems enhance their resilience, thereby augmenting the efficiency and security of the network architecture [17].

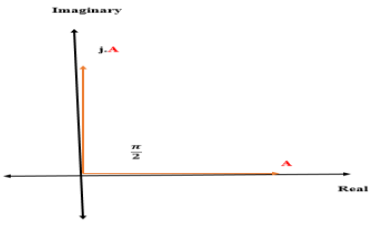

Fig.5 The phasor product

Figure 5 depicts the concept of the phasor product for PAPR reduction. The SLM technique is highly sensitive to changes in the input data, which in turn is highly sensitive to vector multiplications [18]. It can be intuitively inferred that vector multiplications would lead to the change in the way the data blocks add up with each other thereby changing the nature of the time domain transmitted signal. This would change the PAPR of the data stream [19].

If x1, x2 ….. xm are the different vectors, they would result in multiple copies of the data b1, b2… bm. The one with the least PAPR is to be chosen [20].

X=[$x1$ $x2$……xn] is called the shift vector.
For example,
if $x1$=0 $radian, there\ is\ NO\ shift.$
if $x2$=π/2 $radian, there\ is\ a\ shift\ of$ 90 $degrees.$
if $x2$=π $radian, there\ is\ a\ shift\ of$ 180 $degrees.$

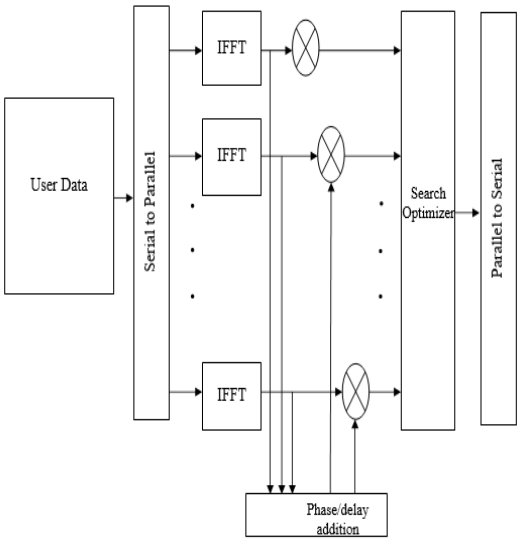

Fig.6 Block diagram for SLM algorithm

Figure 6 depicts the SLM approach. While the SLM approach has high PAPR reduction capability, it suffers from exponential rise in computational complexity as the phase vector length increases. This has prohibited domino-SLM architectures to be used for PAPR reduction [21]-[22].
The SLM technique relies on Vector Multiplications causing shifts in the data signals. However, a trade off exists between the number of complex vectors, crest factor reduction and the search complexity. This work aims at attaining lesser values of crest factor with respect to baseline techniques so as to secure wireless data transmission.

III. PROPOSED METHODOLOGY

The proposed approach in this work is a modified and windowed version of the selective mapping (SLM) technique, addressing the complexity issues of the SLM. The primary aim of this proposed effort is to reduce the Crest Factor of the system [24]. This would indicate the smallest deviation of the signal from the mean power. This guarantees the absence of abrupt signal peaks in the system, rendering them unrecognizable. This would diminish the perceptibility factor, rendering the data challenging for intruders to identify. Given that data privacy and confidentiality are significant concerns, it is important to utilize a minimal crest factor. The selection of the crest factor must be executed judiciously to avoid complicating the system. Data integrity must be preserved at all levels even through the application of chaos [25].

As discussed earlier regarding the SLM approach, different vector products would yield different shifts and hence different PAPR values. The optimizer selects the vector value with the least PAPR [26]. The windowing function can be applied after detecting the residual peaks in the data stream (in time domain) after the SLM is applied. Subsequently the windowed SLM can be implemented. The inverse sync function has been chosen which can be expressed as:

$$Sync_{inv} = \frac{1}{\sin(\pi z)/\pi z} \qquad (2)$$

Here,
$Sync_{inv}$ is the inverted sync function.
$\sin(\pi z)/\pi z$ is the standard definition of the sync function.

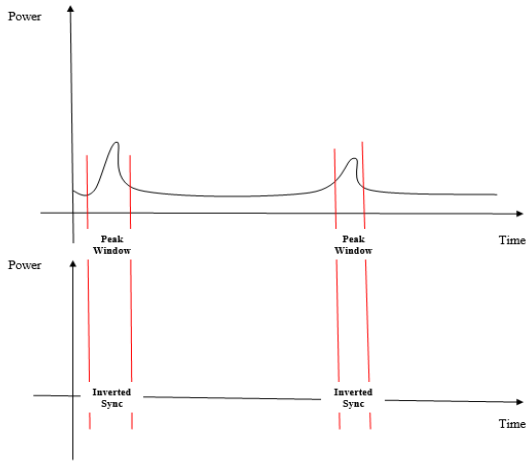

Fig.7 The concept of windowed SLM

Figure 7 exemplifies the windowed SLM. The residual peaks need to be detected after which they can be windowed by the inverted sync function. The proposed algorithm can be presented as:
Start
Step.1: Generate random binary data stream X emulating an actual data transmission environment.
Step.2: Convert the data from serial to parallel employing the transpose operation.

$$Y = X^T \qquad (3)$$

Here,
T denotes the transpose operation.

Step.3: Compute the Fast Fourier Transform of the parallel data.

$$ZZ = FFT(Y) \qquad (4)$$

Step.4: Add different phase or delay vectors to the data stream to generate multiple shifts and hence multiple copies of the data stream with different PAPR values.

$$S_{delay} = [S_1, S_2 \dots \dots \dots S_n] \qquad (5)$$

Step.5: The addition of S_{delay} would result in the generation of multiple copies of the data signal Y expressed as:

$$Y_{composite} = [Y_1, Y_2 \dots \dots \dots Y_n] \qquad (6)$$

Step.6: From $Y_{composite}$ search the copy of the data stream which has the least PAPR i.e.

$$\text{for } i = 1{:}\, n$$
$$\text{find } (\min([Y_1, Y_2 \dots \dots \dots Y_n]))$$

Step.7: Decide the threshold (T) for the residual peaks of the data stream as:

$$T = \text{mean}\{\max(X), \text{mean}(X) \qquad (7)$$

Step.8: Apply the windowing function

$$\text{Sync}_{\text{inv}} = \frac{1}{\sin(\pi z)/\pi z}$$

in the window of the residual peaks.
Step.9: Compute the CCDF of the PAPR.
Stop..

The probability of PAPR reduction can be computed using the complementary cumulative distribution function (ccdf) [27]. The signal is to cross a particular limit or thresholding values in order to cause significant probability of reception which can be mathematically represented as [28]:

$$\text{Prob}\,(Y(t) < Threshold) \quad (8)$$

Here,

Prob stands for probability of reception
Y(t) represents the time domain data stream
Threshold is the value above which perceptibility increases
There are chances where the power of the data stream falls below the threshold of perception. Such a dipping point is called the fading dip of the system. The diagrammatic view of the fading dip is shown in the figure 8. There are chances that fading dips occur in the signal data stream as a function of the time variable. The chances that the signal or the data stream surges pass the fading dip results in reception with minimal errors and the opposite results in exacerbation of errors [29].

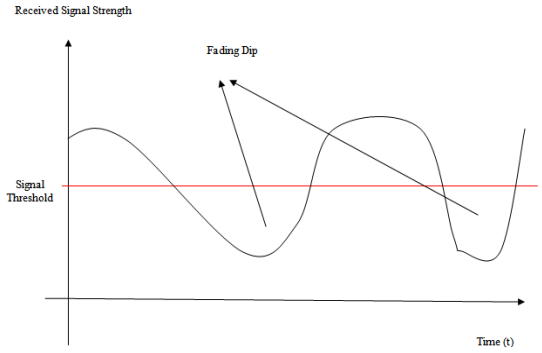

Fig.8 Chances of Fading Dips

The chances of crests arising in the signal are given and analyzed using the PAPR) and can be analyzed using the complementary cumulative distribution function (CCDF) of the system [30].

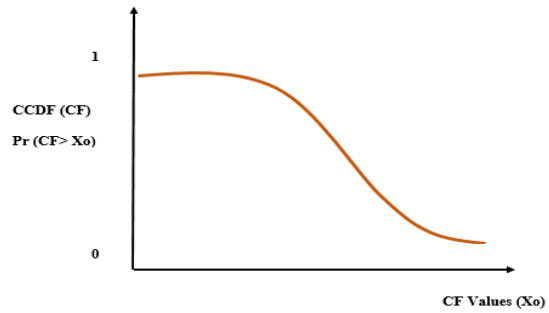

Fig.9 The ccdf curve

Figure 9 depicts the ideal CCDF curve for the PAPR values. It would tend to be asymptotic to the x-axis (PAPR values) in the ideal case. The ccdf is defined as [31]:

$$ccdf(PAPR) = 1 - cdf(PAPR) \quad (9)$$

Lower values of CCDF are desirable to render imperceptibility and security to the data stream.

IV. EXPERIEMNTAL RESULTS

The proposed system has been implemented on MATLAB. A total of 10^6 bits have been used for the simulation. The experimental results obtained through implementing the proposed approach are presented in this section:

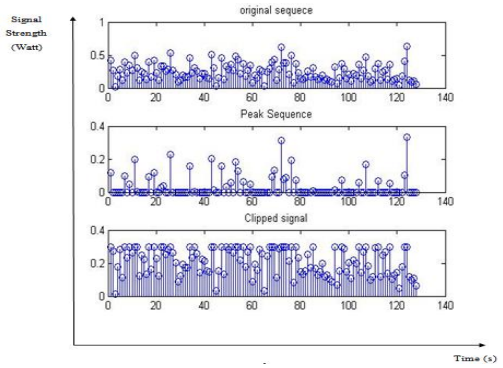

Fig.10 The clipping mechanism

Figure 10 depicts the clipping mechanism in which the signal values above the threshold are clipped. This results in information loss though with the potential benefit of lesser implementation complexity.

The simulation conducted here adds different delay vectors with a separation in 1 degree in the interval of $[0, \frac{\pi}{2}]$ to simulated the SLM, which would yield a pattern of CF or PAPR as a function of phase vectors.

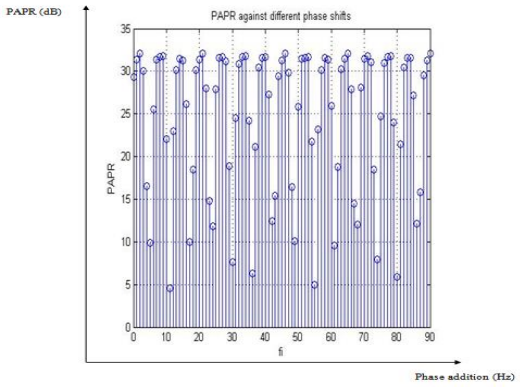

Fig.11 Variation of CF as a function of phase vector

Figure 11 depicts the variation of PAPR for the phase vector variation in the range $[0, \frac{\pi}{2}]$ (in degrees).

It can be observed that there is a random variation in the PAPR values with variations in the phase vectors with no visible pattern thereby making it necessary to implement a searching algorithm to find the phase vector corresponding to the minimal PAPR in the range of the testing added phase vector range.

In this particular case, 11 degree happens to be the vector resulting in least PAPR value. For a phase vector length in the range $U = [1, 2, 4, 8, 16]$, the variation in the PAPR can be observed. Such a vector with phase vector lengths is a more practical approach for wireless networks which can have data transfer rates in 100s of Mbps or Gbps.

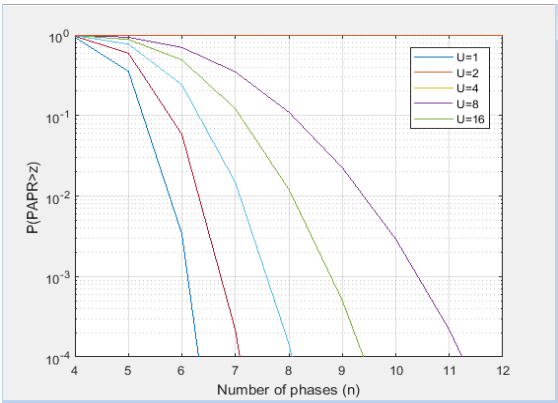

Fig.12 Variation of CF as a function of phase vector

Figure 12 depicts the variation in the PAPR as a function of vector length in this case (not actual vector values, but length). It can be observed that increasing the vector length increases the probability (ccdf) of PAPR reduction continuously, but the con would be the increasing search complexity of the system.

The application of SLM is bound to reduce the PAPR of the system thereby reducing the perceptibility of data transfer to adversaries. However, the SLM would not make the CF or PAPR equal to unity. The residual peaks in the present data stream (in time domain) would pose a challenge in creating the imperceptibility. Thus a time domain analysis for the data stream subsequent to analysis of SLM needs to be done.

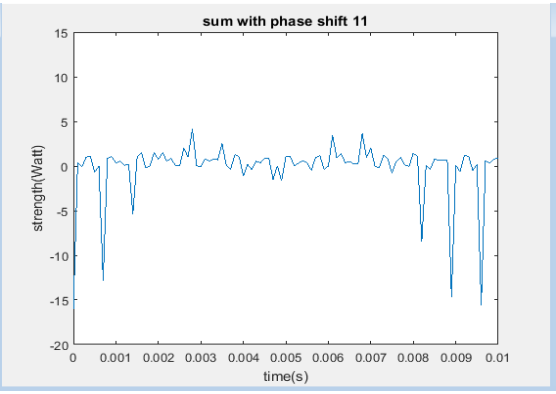

Fig.13 Residual peaks at least CF phase vector chosen

Figure 13 depicts the residual peaks corresponding to the chosen phase vector that is chosen in the range of $[0, \frac{\pi}{2}]$ (in degrees). The residuals happen to reduce the perceptibility. Hence, windowing approach is necessary.

The data transmission mechanism for the proposed technique has been chosen as OFDM for its wide applicability in wireless networks. This multiple access technique is well suited for large and wide area wireless networks catering to multiple users constrained in frequency domain (bandwidth)

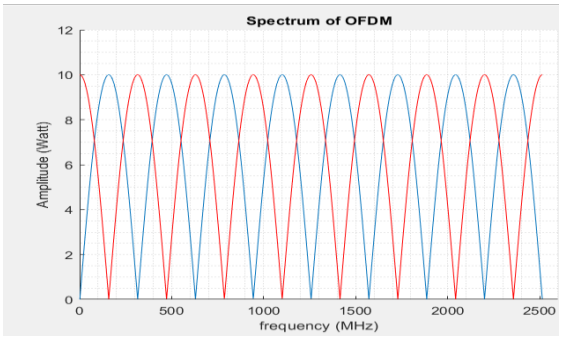

Fig.14 Data signal spectrum

Figure 14 depicts the signal spectrum depicting the orthogonality among carriers. It can be observed that the carriers seem to overlap but interference is avoided as one carrier is at its zero crossing when the other one is at its maximum.

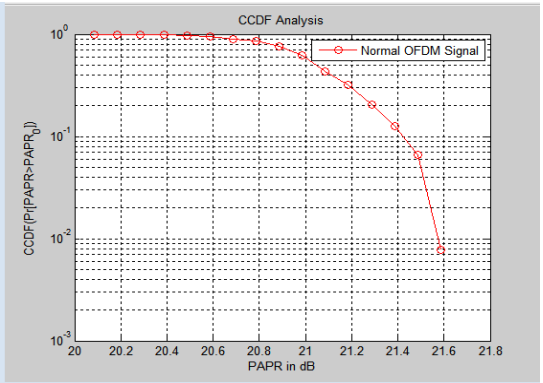

Fig.15 CCDF of data stream with OFDM as multiple access

Figure 15 depicts the CCDF of the data stream with OFDM as the multiple access technique. It can be observed that the least value of PAPR achieved in this case is around 21.5dB.

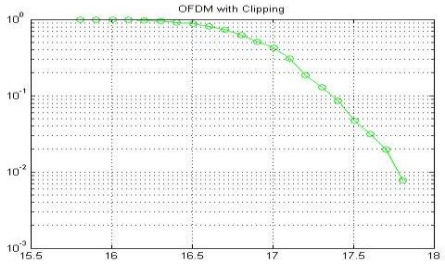

Fig.16 CCDF of data stream with Clipped-OFDM as multiple access

Figure 16 depicts the CCDF of the data stream with Clipped-OFDM as the multiple access technique. It can be observed that the least value of PAPR achieved in this case is around 17.8dB.

A clear difference in the PAPR value compared to original data stream can be observed with clipping, but this comes at the cost of information loss of the data stream. It can however be easily implemented on software defined networks with threshold settings.

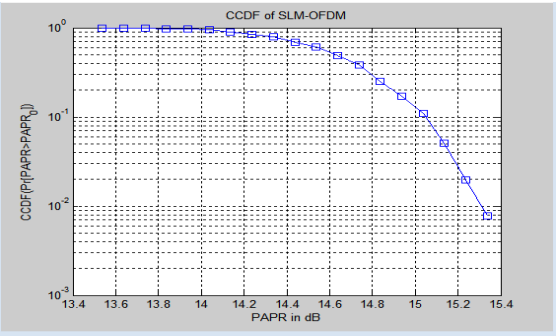

Fig.17 CCDF of data stream with SLM as multiple access

Figure 17 depicts the CCDF of the data stream with SLM-OFDM as the multiple access technique. It can be observed that the least value of PAPR achieved in this case is around 15.4dB. Thus the SLM based approach can be seen to attain a lower PAPR value compared to the clipping technique sans the information loss attribute.

However, the search complexity remains the major challenge in this case. The further reduction of the PAPR can be done based on the windowing function used in conjugation with the SLM approach.

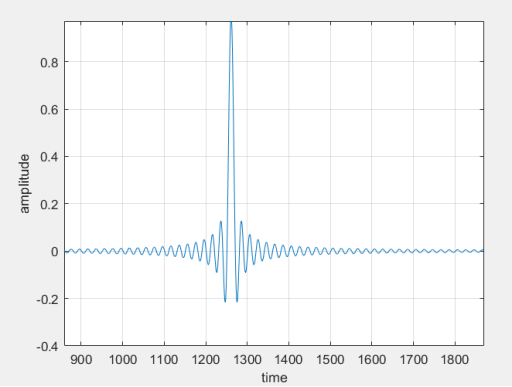

Fig.18 Implementing the sync window

Figure 18 depicts the sync window that is to be inverted and applied to the residual peaks. While other windowing functions could be used, the one with the similarity with the actual data streams after modulation has been chosen.

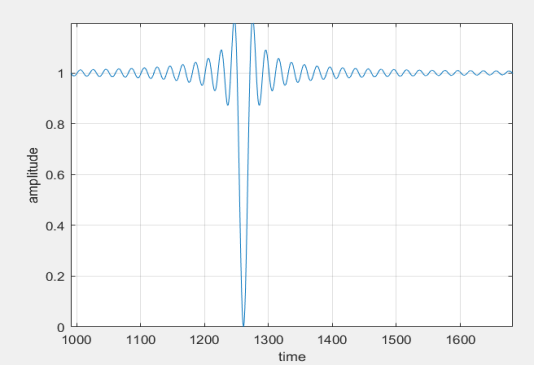

Fig.19 Implementing the inverted sync window

Figure 19 depicts the inverted sync window implemented on residual peaks of the SLM.

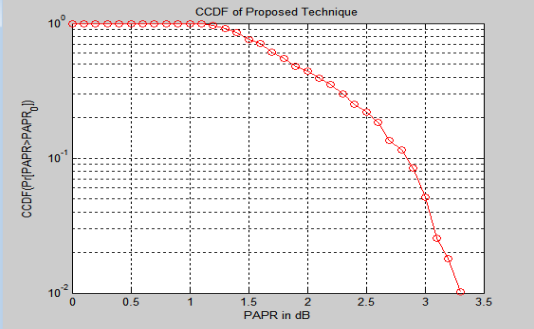

Fig.20 CCDF of data stream with windowed-SLM OFDM as multiple access

Figure 20 depicts the CCDF analysis of the proposed approach which uses the inverse sync as the windowing function alongside the SLM based approach.

It can be clearly observed that the PAPR reduces to around 3.4 dB if the proposed approach is used. This would significantly reduce the perceptibility of the data stream for adversaries.

A comparative analysis of the obtained CCDF of the PAPR for the various techniques is presented in table 1.

Table 1. Comparative CCDF (PAPR) values for different techniques.

S.No.	Technique	PAPR value
1.	Original data stream	21.5
2.	Clipping Approach	17.8
3.	SLM	15.4
4.	Proposed Windowed SLM	3.4

It can be clearly observed from table 1 that the windowed SLM approach attains the highest PAPR reduction among all simulated approaches and hence the PAPR of the proposed approach has the least value of PAPR resulting in highest security.

Another important aspect of the SLM algorithm which needs to be investigated is the PAPR reduction capability of the algorithm as a function of vector length. It is tabulated in table 2.

Table 2. PAPR variation with SLM vector length

S.No.	Vector length	PAPR value
1.	2	9.5
2.	4	8
3.	8	7.1
4.	16	6.3

Table 2 clearly shows the PAPR reduction capability of the SLM approach as the length of the phase vector increases.

The results of the proposed system clearly indicate the fact that the proposed system outperforms the clipping and the selective mapping based approaches in terms of the PAPR reduction capability.

V. CONCLUSION

Conventional NIDS based approaches are being threatened through emerging technologies such as AI and quantum computing. Proactive network-level security can be substantially improved using PAPR reduction methods. Enhancing signal transmission efficiency and mitigating vulnerabilities linked to high PAPR enables networks to more effectively anticipate and avert potential security threats. Integrating PAPR reduction measures into the design and administration of communication systems enhances network infrastructure security and reliability, protecting data transmission and overall system performance. The previous discussions throw light on the design of a proactive approach to secure wireless networks, based on the reduction of PAPR of the data stream to be transmitted. The approach leverages the low PAPR values of the data stream to create imperceptibility of the transmitted data thereby shrouding the data transmission from an adversarial point of view. The various techniques commonly employed for reducing the PAPR of the data transfer have been discussed and implemented. The pros and cons of the approaches have been discussed too. Further, a windowed SLM algorithm has been conceptualized and implemented. The results clearly demonstrate the fact that the windowed SLM attains much lesser PAPR value compared to the other commonly used approaches. Thus, the proposed approach can serve as an effective proactive security mechanism for wireless networks.

While the SLM can be shown to have an exceptional PAPR reduction capability without rendering any data loss, it can be further enhanced using the partitioning of the data blocks and subsequently adding the phase vectors. Such an approach with sub-partitioning of code block can render further reduction of the PAPR of the system, at the cost of adding complexity to the system. With advancements in chip design and fabrication, it is expected that more complex algorithms would turn out to be feasible in the near future. Thus this aspect explored as a future enhancement of the proposed work.

REFERENCES

[1] T. Hurley, J. E. Perdomo and A. Perez-Pons, "HMM-Based Intrusion Detection System for Software Defined Networking," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), 2016, pp. 617-621.

[2] D. Wulich, "Definition of efficient PAPR in OFDM," in IEEE Communications Letters, 2005, vol. 9, no. 9, pp. 832-834.

[3] Y. A. Jawhar et al., "A Review of Partial Transmit Sequence for PAPR Reduction in the OFDM Systems," in IEEE Access, 2019, vol. 7, pp. 18021-18041

[4] Mohamad F. Haroun, T. Aaron Gulliver, "Secure OFDM with Peak-to-Average Power Ratio Reduction Using the Spectral Phase of Chaotic Signals", Entropy, MDPI 2021, vol.23, issue.1380, pp.1-15.

[5] J. Shen Bo Liu; Yaya Mao; Rahat Ullah; Jianxin Ren; Jianye Zhao; Shuaidong Chen., "Enhancing the Reliability and Security of OFDM-PON Using Modified Lorenz Chaos Based on the Linear Properties of FFT," in Journal of Lightwave Technology, vol. 39, no. 13, pp. 4294-4299, July1, 2021.

[6] S. -B. Ryu, J. -H. Choi, J. Bok, H. Lee and H. -G. Ryu, "High Power Efficiency and Low Nonlinear Distortion for Wireless Visible Light Communication," 2011 4th IFIP International Conference on New Technologies, Mobility and Security, 2011, pp. 1-5.

[7] F. S. Shawqi, L. Audah, A. T. Hammoodi, M. M. Hamdi and A. H. Mohammed, "A Review of PAPR Reduction Techniques for UFMC Waveform," 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020, pp. 1-6

[8] S. Gökceli et al., "Novel Iterative Clipping and Error Filtering Methods for Efficient PAPR Reduction in 5G and Beyond," in IEEE Open Journal of the Communications Society, 2021, vol. 2, pp. 48-66.

[9] B. Tang, K. Qin and H. Mei, "A Hybrid Approach to Reduce the PAPR of OFDM Signals Using Clipping and Companding," in IEEE Access, 2020, vol. 8, pp. 18984-18994.

[10] R Niwareeba, MA Cox, L Cheng, "Low complexity hybrid SLM for PAPR mitigation for ACO OFDM", ICT Express, Elsevier 2022, vol.8, no.1, pp.72-76.

[11] R. Niu and L. Wang, "Double-Optimal PTS Scheme for PAPR Reduction in OFDM Systems," 2021 IEEE 21st International Conference on Communication Technology (ICCT), 2021, pp. 198-202.

[12] J. Shen et al., "Enhancing the Reliability and Security of OFDM-PON Using Modified Lorenz Chaos B.ased on the Linear Properties of FFT," in Journal of Lightwave Technology, 2021, vol. 39, no. 13, pp. 4294-4299

[13] Z. S. Al-Aubaidy and S. M. Ali, "Low PAPR OFDM with implicit side information and reduced complexity for IOT networks," 2018 Advances in Science and Engineering Technology International Conferences (ASET), 2018, pp. 1-6.

[14] J. Li, X. Zeng, C. Yin, Q. Luo and G. Li, "A Low-Complexity CRC-Based Decoding Algorithm for SLM-ML OFDM Systems," in IEEE Wireless Communications Letters, 2021, vol. 10, no. 6, pp. 1144-1147.

[15] V. Savaux and Y. Louét, "PAPR Analysis as a Ratio of Two Random Variables: Application to Multicarrier Systems With Low Subcarriers Number," in IEEE Transactions on Communications, 2018, vol. 66, no. 11, pp. 5732-5739.

[16] Mohamad F. Haroun, T. Aaron Gulliver, "Secure OFDM with Peak-to-Average Power Ratio Reduction Using the Spectral Phase of Chaotic Signals", Entropy, MDPI 2021, vol.23, issue.1380, pp.1-15.

[17] SR Moosavi, TN Gia, AM Rahmani, E Nigussie, "SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways", Procedia Computer Science, Elsevier 2015, vol. 52, pp. 452-459.

[18] S. Sathyadevan, Vejesh V, R. Doss and L. Pan, "Portguard - an authentication tool for securing ports in an IoT gateway," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 624- 629.

[19] A. Olutayo, J. Cheng and J. F. Holzman, "A New Statistical Channel Model for Emerging Wireless Communication Systems," in IEEE Open Journal of the Communications Society, vol. 1, pp. 916-926, 2020.

[20] A. Albaseer, B. S. Ciftler and M. M. Abdallah, "Performance Evaluation of Physical Attacks against E2E Autoencoder over Rayleigh Fading Channel," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 177-182

[21] E. Björnson and L. Sanguinetti, "Rayleigh Fading Modeling and Channel Hardening for Reconfigurable Intelligent Surfaces," in IEEE Wireless Communications Letters, vol. 10, no. 4, pp. 830-834, April 2021.

[22] S. Yousefi, H. Narui, S. Dayal, S. Ermon and S. Valaee, "A Survey on Behavior Recognition Using WiFi Channel State Information," in IEEE Communications Magazine, vol. 55, no. 10, pp. 98-104, Oct. 2017.

[23] C. Studer, S. Medjkouh, E. Gonultaş, T. Goldstein and O. Tirkkonen, "Channel Charting: Locating Users Within the Radio Environment Using Channel State Information," in IEEE Access, vol. 6, pp. 47682-47698, 2018.

[24] A. Saci, A. Al-Dweik, A. Shami and Y. Iraqi, "One-Shot Blind Channel Estimation for OFDM Systems Over Frequency-Selective Fading Channels," in IEEE Transactions on Communications, vol. 65, no. 12, pp. 5445-5458, Dec. 2017.

[25] W. Ma, C. Qi and G. Y. Li, "High-Resolution Channel Estimation for Frequency-Selective mmWave Massive MIMO Systems," in IEEE Transactions on Wireless Communications, vol. 19, no. 5, pp. 3517-3529, May 2020

[26] K. Venugopal, N. González-Prelcic and R. W. Heath, "Optimality of Frequency Flat Precoding in Frequency Selective Millimeter Wave Channels," in IEEE Wireless Communications Letters, vol. 6, no. 3, pp. 330-333, June 2017.

[27] A. Kumar, N. Gaur and A. Nanthaamornphong, "Optimizing PAPR, BER, and PSD Efficiency: Using Phase Factors Generated by Bacteria Foraging Algorithm for PTS and SLM Methods," in IEEE Access, 2024, vol. 12, pp. 54964-54977

[28] P. Singh, E. Sharma, K. Vasudevan and R. Budhiraja, "CFO and Channel Estimation for Frequency Selective MIMO-FBMC/OQAM Systems," in IEEE Wireless Communications Letters, vol. 7, no. 5, pp. 844-847, Oct. 2018.

[29] R. Zayani, J. -B. Doré, B. Miscopein and D. Demmer, "Local PAPR-Aware Precoding for Energy-Efficient Cell-Free Massive MIMO-OFDM Systems," in IEEE Transactions on Green Communications and Networking, 2023, vol. 7, no. 3, pp. 1267-1284.

[30] M Bharti, “Analysis of PAPR suppression scheme for next generation wireless system”, International Journal of System Assurance Engineering and Management, Springer 2023, vol.14, pp. 818–826.