A Review on Proactive Security Through PAPR Reduction in Web 3.0 and IOT Networks

Anil Kumar Yadav[1], Prof. Pawan Panchole[2]
VITM, Indore[1,2]

ABSTRACT: With increasing number of cellular network users, large data being generated and limited bandwidth available for systems, efficient multiplexing techniques are needed that use the available bandwidth efficiently for IoT and Web 3.0 Systems. It is widely used in cellular and internet of things (IoT) based applications. One of the major challenges that IoT suffers from is high value of Peak to Average Power Ratio (PAPR), which reduces its security. High PAPR causes high level of perceptibility and low security. Hence it is necessary to reduce the PAPR of the OFDM systems. Several techniques have been employed so far for the reduction of PAPR in IoT systems. This paper presents a review on the most common PAPR reduction techniques for OFDM systems.

Keywords: Computer Networks, IoT, Peak to Average Power Ratio (PAPR), PAPR reduction.

I. INTRODUCTION

For any bandwidth constrained cellular system, the bandwidth would be limited, hence an effective multiplexing technique is needed [1]. Thus, OFDM is widely chosen as the multiplexing technique for several applications such as cellular networks, IoT, Local Area Networks (LANs), WiMax etc. While transmitting the OFDM based IoT data, it is mandatory to ensure high reliability (Quality of Service) by reducing the BER value. However, this a severely challenging with fading condition and high power amplifiers need to be used to boost the OFDM signals. Hence, it is necessary to reduce the PAPR of the system to avoid the distortions in the finally received OFDM signal to maintain high reliability and Quality of Service [2].

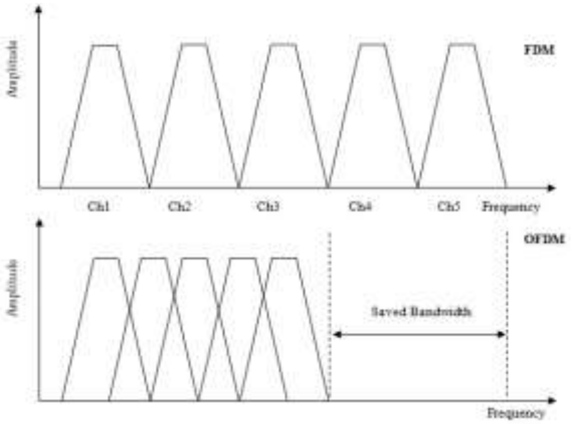

Fig.1 Spectra of FDM and OFDM for Web 3.0 Networks

Figure 1 shows the spectra of OFDM and FDM (frequency division multiplexing). It can be seen that OFDM helps to save critically important bandwidth. Use of OFDM has 2 benefits [3]:

1. The saved bandwidth can be used to accommodate more users
2. The saved bandwidth can be distributed among users to provide them with more bandwidth.
3. Higher bandwidth per user means high speed of data transfer [4].

Physical layer security aims to secure wireless communication by exploiting the inherent randomness of wireless channels [5]. High PAPR signals may become predictable or exhibit patterns that can be exploited by adversaries performing signal reconstruction or constellation analysis. Conversely, controlled PAPR reduction techniques such as clipping, coding, tone reservation, or selective mapping can introduce intentional randomness or reduce exploitable signal artifacts, thereby improving secrecy capacity. Hence, PAPR reduction contributes to making the transmitted waveform statistically unpredictable to an eavesdropper [6].

II. PEAK TO AVERAGE POWER RATIO (PAPR) AND SECURITY

In wireless networks, eavesdroppers often rely on sophisticated signal processing schemes to recover transmitted symbols even under noisy conditions. High PAPR signals, when distorted by nonlinear amplifiers, create spectral regrowth that may inadvertently expose useful information to attackers [7]. PAPR reduction minimizes this distortion, thereby reducing information leakage. Moreover, schemes like Selective Mapping (SLM) and Partial Transmit Sequence (PTS) use pseudorandom phase sequences, which inherently function as additional cryptographic layers: without the phase sequence key, an eavesdropper cannot reconstruct the original OFDM symbol precisely, strengthening waveform-level security.

The peak to average power ratio (PAPR) of the system is defined as the ratio of the peak power to that of the average power of the system Mathematically, it is defined as [8]

$$PAPR = \frac{\max\{X(t)^2\}}{mean\,\{X(t)^2\}} \tag{1}$$

Here,

PAPR stands for peak to average power ratio

X(t) is the transmitted signal

Max represents the peak of the signal

Mean represents the average value

The significance of this term lies in the fact that the PAPR gives the deviation of the signal from the average power thereby making higher distortions in High Power Amplifiers (HPAs). OFDM inherently suffers from high PAPR which results in increased errors at the receiving end of networks. Thus it is necessary to reduce the PAPR of the system [9].

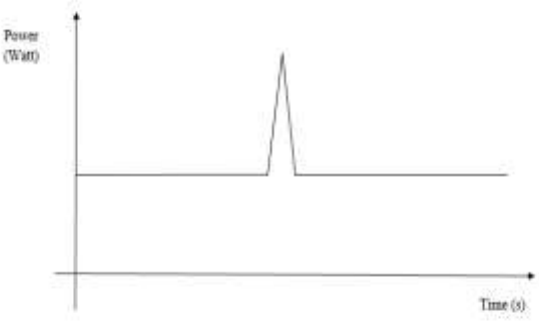

Fig.2 Graphical representation of PAPR

Figure 2 shows the graphical representation of PAPR of the system where the peak power greatly exceeds the average power.

Low-power wireless networks such as IoT, WBANs, and sensor networks are particularly sensitive to PAPR issues because their power amplifiers operate with narrow linearity margins. High PAPR forces these devices to operate with higher back-off, increasing energy consumption and making them vulnerable to side-channel attacks that track power fluctuations. PAPR reduction ensures stable power consumption and reduces unintended electromagnetic emissions, making it more difficult for attackers to infer transmitted data using RF fingerprinting or power-analysis attacks. Consequently, PAPR reduction becomes an integral part of lightweight security for resource-constrained devices [10].

III. RELATED WORK

This section presents the major noteworthy contribution in the domain of research on PAPR reduction in OFDM systems in tabular form.

S.No	Authors	Approach	Publication
1.	Padave et al. [11]	Qualitative Analysis on Implementation of Security Aspects for Web 3.0	IEEE 2025
2.	Kumar et al. [12]	Optimizing PAPR, BER, and PSD Efficiency: Using Phase Factors	IEEE 2024

		Generated by Bacteria Foraging Algorithm for PTS and SLM Methods	
3.	Luo et al. [13]	Robust Key Update With Controllable Accuracy Using Support Vector Machine for PONs	IEEE 2023
4.	Lv et al. [14]	Genetic Algorithm (GA) based partially transmitted sequences (PTS) algorithm for PAPR reduction.	IEEE 2022
5.	Gopi et al. [15]	Optimized Selective Mapping through hybrid of linear integer programming (LIP) and Selective Mapping (SLM)	IEEE 2021
6.	Aghdam et al. [16]	Combination of Particle Swarm Optimization (PSO) and Partially Transmitted Sequences (PTS) for PAPR reduction.	Elsevier 2019.
7.	Rao et al. [17]	PTS and grey wolf optimization hybrid algorithm for PAPR reduction.	Springer 2019.
8.	Zaid et al. [18]	Low PAPR OFDM with Implicit Side Information and reduced Complexity for IoT Networks	IEEE 2018
9.	Sultan et al. [19]	Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON	IEEE 2018
10.	Adnan et al. [20]	Chaotic Walsh–Hadamard Transform for Physical Layer Security in OFDM-PON	IEEE 2017
11.	Zhang et al. [20]	Physically Secured Optical OFDM by Employing Chaotic Pseudorandom RF Subcarriers	IEEE 2107

Table.1 Existing Approaches for PAPR reduction

IV. CCDF FOR PAPR ANALYSIS

The Peak to Average Power Ratio (PAPR) can be analyzed using a probability function called the Complementary Cumulative Distribution Function or CCDF. Mathematically CCDF for PAPR can be defined as [21]:

$$y = Prob\,(PAPR > PAPR_0) \qquad (2)$$

The CCDF of the PAPR denotes the probability that the PAPR of a data block exceeds a given threshold $PAPR_0$.

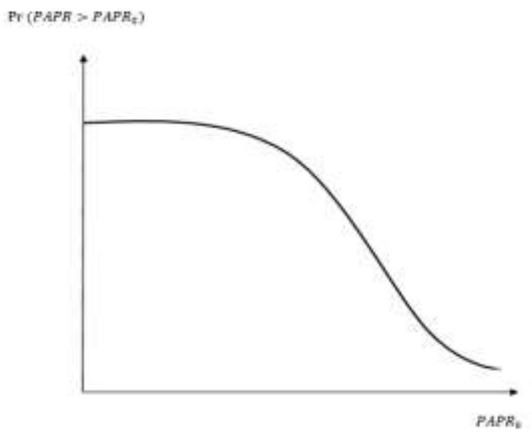

Fig.3 Typical PAPR CCDF graph for OFDM systems

Figure 3 shows a typical CCDF graph for the PAPR analysis. The graphs shows that as the value of PAPR increases, the chances or probability that the system PAPR would exceed the threshold PAPR reduces. A quick drop in the CCDF graph for low values of PAPR is desirable.

Web 3.0 envisions a decentralized internet built on blockchain, edge intelligence, distributed data ownership, and immersive digital applications such as metaverse platforms. To support these emerging use cases, wireless networks must deliver ultra-reliable, energy-efficient, high-capacity communication. Technologies like OFDM dominate 5G/6G systems due to their spectral efficiency and flexibility, but they suffer from a major drawback—high Peak-to-Average Power Ratio (PAPR). Reducing PAPR becomes essential in Web 3.0 infrastructures to ensure sustainable device operation, secure communication, and high-quality user experiences [22]

Despite its advantages, PAPR reduction must be carefully balanced with computational overhead and potential bit error rate (BER) degradation. Techniques like SLM and PTS require additional side information to be transmitted, and if this side information is intercepted, security may be compromised. Similarly, clipping-based schemes may introduce in-band distortion if not properly filtered. Therefore, designers must select PAPR reduction techniques not merely for performance improvement but for their ability to enhance physical layer security without imposing excessive overhead [23].

V. CONCLUSION

It can observed that IoT applications are bandwidth constrained. IoT networks suffers from the problem of high PAPR. It is necessary to reduce PAPR and also ensure no or very data loss. High PAPR leads to power inefficiency, signal distortion, and increased vulnerability to eavesdropping because nonlinearities in power amplifiers can unintentionally leak side information. Recently, researchers have started viewing PAPR not only as a performance issue but also as a security parameter because of its potential influence on the confidentiality and detectability of transmitted signals. This paper presents a review on the fundamentals of IoT along with the problem of PAPR. The various PAPR reduction techniques used in contemporary work have also been cited, for proactive security.

References

1. L. Jain and N. Joshi, "Impacts of Web 3.0 on Cyber Security: Challenges and Countermeasures," 2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit), Greater Noida, India, 2024, pp. 912-917.
2. J Zhu, F Li, J Chen, “A survey of blockchain, artificial intelligence, and edge computing for Web 3.0”, Computer Science Review, Elsevier, 2024, vol.54, 100667.
3. 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
4. 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.

5. 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.

6. 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.

7. 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

8. 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.

9. 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.

10. 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.

11. S. Padave, N. A. Natraj and G. G. Hallur, "Qualitative Analysis on Implementation of Security Aspects for Web 3.0," IEEE Internet of Things Journal, vol.16., pp. 1352-1356.

12. 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

13. Y. Luo, C. Zhang, X. Wang, X. Liang and K, Kiu, “Robust Key Update With Controllable Accuracy Using Support Vector Machine for Secure OFDMA-PON”, Journal of Lightwave Technology, IEEE, 2023, vol. 41, no. 14, pp. 4663-4671.

14. S. Lv, J. Zhao, L. Yang and Q. Li, "Genetic Algorithm Based Bilayer PTS Scheme for Peak-to-Average Power Ratio Reduction of FBMC/OQAM Signal”, IEEE 2021.

15. S. Gopi and S. Kalyani, "An Optimized SLM for PAPR Reduction in Non-Coherent OFDM-IM”, IEEE 2020.

16. MH Aghdam, AA Sharifi, “PAPR reduction in OFDM systems: An efficient PTS approach based on particle swarm optimization”, Elsevier 2019.

17. RS Suriavel Rao, P Malathi, “A novel PTS: grey wolf optimizer-based PAPR reduction technique in OFDM scheme for high-speed wireless applications” Springer 2019.

18. Zaid S. Al-Aubaidy, Saloa M. Ali,“ Low PAPR OFDM with Implicit Side Information and reduced Complexity for IoT Networks.”, IEEE 2018

19. Amber Sultan ,Xuelin Yang , Adnan A. E. Hajomer ,Weisheng Hu,“ Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON”, IEEE 2018

20. Adnan A. E. Hajomer , Xuelin Yang ,Weisheng Hu, “Chaotic Walsh–Hadamard Transform for Physical Layer Security in OFDM-PON”, IEEE 2017

21. Chongfu Zhang ,Wei Zhang , Xiujun He , Chen Chen ; Huijuan Zhang ; Kun Qiu, , “Physically Secured Optical OFDM by Employing Chaotic Pseudorandom RF Subcarriers”, IEEE 2017.

22. K. Vayadande, A. Baviskar, J. Avhad, S. Bahadkar, P. Bhalerao and A. Chimkar, "A Comprehensive Review on Navigating the Web 3.0 Landscape," 2024 Second International Conference on Inventive Computing and Informatics (ICICI), Bangalore, India, 2024, pp. 456-463

23. 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.