A Review on Proactive Security Approaches for Web 3.0 and IoT Networks through Chaos

Darshan Kusmakar[1] Prof. Virendra Verma[2]

ABSTRACT: Web 3.0, with its focus on decentralization and interoperability, introduces novel security challenges that require careful consideration. In this context, it's essential to address the security issues associated with the evolution of the Semantic Web. Decentralization, a core principle of Web 3.0, introduces security concerns related to the use of blockchain technology. While blockchain enhances transparency and tamper resistance, it's not immune to vulnerabilities. Smart contract exploits, consensus algorithm weaknesses, and the potential for 51% attacks on decentralized networks are among the specific security threats that must be addressed to ensure the robustness of decentralized systems. One of the major challenges such networks 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 systems. Several techniques have been employed so far for the reduction of PAPR in systems. This paper presents a review on the most common PAPR reduction techniques.

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

I. INTRODUCTION

Web 3.0, often referred to as the Semantic Web, represents the next evolution of the World Wide Web. Unlike its predecessor, Web 2.0, which focused on user-generated content and social collaboration, Web 3.0 aims to bring a more intelligent and interconnected online experience. This new phase envisions a web where machines can understand and interpret data, making it more accessible and meaningful for users. Interoperability is a key focus of Web 3.0, aiming to create a seamless and interconnected digital experience. This involves breaking down silos of information by enabling diverse applications and platforms to communicate and share data effectively. The goal is to enhance user experiences by providing a unified and integrated online environment. Highlight the importance of interoperability in Web 3.0, showcasing how it differs from the current fragmented digital landscape. Emphasize the user-centric benefits of a more interconnected web.

Fig.1 Web 3.0

Decentralization is another fundamental aspect of Web 3.0, aiming to reduce reliance on centralized entities and empower users with greater control over their data. Blockchain technology plays a significant role in achieving decentralization, ensuring transparency, security, and trust in online interactions.

II. PROACTIVE SECURITY AND PAPR

The common security mechanism is employing application level / bit level encryption algorithms. However, with the increasing computational capability of machines based on AI and Quantum Computing, Encryption alone CAN NOT prove to be completely secure. The above argument makes it necessary to implement algorithms which can make the data transmission Imperceptible.

This can be done by employing chaos and keeping the crest factor of the data transmission as low as possible 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:

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

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.

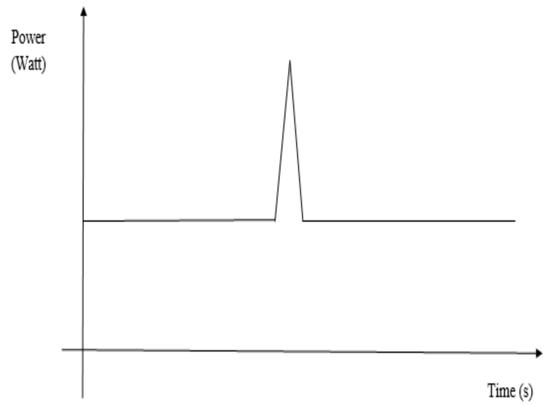

Fig.2 Graphical representation of PAPR

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

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.	Robust Key Update With Controllable Accuracy Using Support Vector Machine for Web 3.0	IEEE 2023
1.	Zaid et al.	A Selective Mapping Based Technique for PAPR reduction for IoT Networks	IEEE 2021
2.	Lv et al.	Genetic Algorithm (GA) based partially transmitted sequences (PTS) algorithm for PAPR reduction.	IEEE 2020
3.	Gopi et al.	Optimized Selective Mapping through	IEEE 2020

		hybrid of linear integer programming (LIP) and Selective Mapping (SLM)	
4.	Aghdam et al.	Combination of Particle Swarm Optimization (PSO) and Partially Transmitted Sequences (PTS) for PAPR reduction.	Elsevier 2019.
5.	Rao et al.	PTS and grey wolf optimization hybrid algorithm for PAPR reduction.	Springer 2019.
6.	Xiao et al.	Low PAPR OFDM with Implicit Side Information and reduced Complexity for IoT Networks	IEEE 2018
7.	Sultan et al.	Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON	IEEE 2018
8.	Adnan et al.	Chaotic Walsh–Hadamard Transform for Physical Layer Security in OFDM-PON	IEEE 2017
9.	Zhang et al.	Physically Secured Optical OFDM by Employing Chaotic Pseudorandom RF Subcarriers	IEEE 2107
10.	Wei Zhang et al.	Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON	IEEE 2016
11.	Chongfu Zhang et al.	Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in OFDM based IOT systems	IEEE 2016
12.	Hu et al.	Chaos-OFDM based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON	IEEE 2015

13.	Yang et al.	Chaotic signal scrambling for physical layer security in OFDM-PON	IEEE 2015
14.	Liu et al.	Physical Layer Security in OFDM based on Dimension-Transformed Chaotic Permutation	IEEE 2014
15.	Wei Zhang et al.	Chaos Coding-OFDM based IoT QAM IQ-Encryption for Improved Security in OFDMA-PON	IEEE 2014

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:

$$y = Prob\ (PAPR > PAPR_0) \quad (2)$$

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

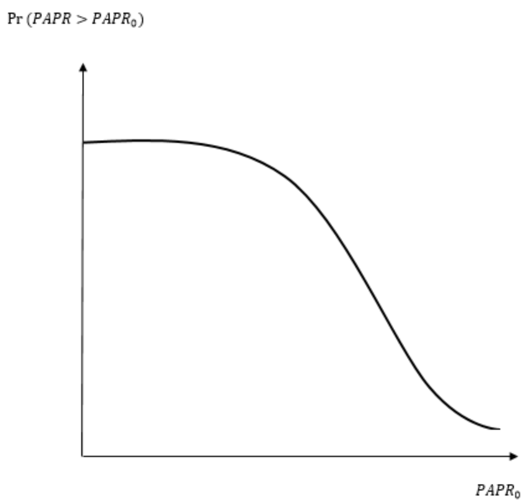

Fig.3 Typical PAPR CCDF graph for OFDM systems

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.

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. 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. S. Padave, N. A. Natraj and G. G. Hallur, "Qualitative Analysis on Implementation of Security Aspects for Web 3.0," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 1352-1356.
2. Zaid S. Al-Aubaidy, “Low PAPR OFDM with Implicit Side Information and reduced Complexity for IoT Networks”, IEEE 2022

3. 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.
4. S. Gopi and S. Kalyani, "An Optimized SLM for PAPR Reduction in Non-Coherent OFDM-IM", IEEE 2020.
5. MH Aghdam, AA Sharifi, "PAPR reduction in OFDM systems: An efficient PTS approach based on particle swarm optimization", Elsevier 2019.
6. 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.
7. Zaid S. Al-Aubaidy, Saloa M. Ali," Low PAPR OFDM with Implicit Side Information and reduced Complexity for IoT Networks.", IEEE 2018
8. Amber Sultan ,Xuelin Yang , Adnan A. E. Hajomer ,Weisheng Hu," Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON", IEEE 2018
9. Adnan A. E. Hajomer , Xuelin Yang ,Weisheng Hu, "Chaotic Walsh–Hadamard Transform for Physical Layer Security in OFDM-PON", IEEE 2017
10. Chongfu Zhang ,Wei Zhang , Xiujun He , Chen Chen ; Huijuan Zhang ; Kun Qiu, , "Physically Secured Optical OFDM by Employing Chaotic Pseudorandom RF Subcarriers", IEEE 2017
11. Wei Zhang ,Chongfu Zhang ,Chen Chen ,Wei Jin ,Kun Qiu, "Joint PAPR Reduction and Physical Layer Security Enhancement in OFDMA-PON",IEEE 2016
12. Wei Zhang ,Chongfu Zhang ,Wei Jin ,Kun Qiu ,Chen Chen," Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in OFDM based IOT systems", IEEE 2016
13. Xiaonan Hu , Xuelin Yang , Zanwei Shen ,Hao He ,Weisheng Hu ,Chenglin Bai," Chaos-OFDM based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON",IEEE 2015
14. Xuelin Yang , Xiaonan Hu ,Zanwei Shen ,Hao He ,Weisheng Hu ,Chenglin Bai, "Chaotic signal scrambling for physical layer security in OFDM-PON",IEEE 2015
15. Bo Liu ,Lijia Zhang ,Xiangjun Xin ,Yongjun Wang," Physical Layer Security in OFDM based on Dimension-Transformed Chaotic Permutation", IEEE 2014
16. Wei Zhang ; Chongfu Zhang ; Wei Jin ; Chen Chen ; Ning Jiang ; Kun Qiu," Chaos Coding-OFDM based IoT QAM IQ-Encryption for Improved Security in OFDMA-PON", IEEE 2014