ISSN 2319-5991 www.ijerst.com

Peer Reviewed,Referred & Indexed Journal

Research Paper

DESIGN AND SIMULATION OF HARDWARE-BASED ETHERNET MAC FIREWALL FOR INDUSTRIAL NETWORKS

J. VIDHYA VARDHINI, J. ABHISHEK, K. JHANSI, G. SRAVAN KUMAR

Dr. J. SUNITHA KUMARI

Associate Professor, Department of Electronics and Communication Engineering

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY AUTONOMOUS
(Affiliated to JNTUH, Accredited By NBA, Accredited by NAAC with "A+" grade)
2025-2026

ABSTRACT

Industrial networks such as SCADA and Industrial Control Systems (ICS) require secure and reliable communication while maintaining strict timing constraints. With the increasing use of Ethernet-based communication in these systems, the risk of cyber threats such as unauthorized access and malicious data transmission has significantly increased. Traditional software-based firewalls are not well-suited for such environments, as they introduce variable delays that can affect real-time operations. This project presents the design and simulation of an Ethernet MAC firewall intended for industrial networks. The proposed system integrates packet filtering functionality with the Ethernet Media Access Control (MAC) layer to enable real-time inspection and control of network traffic. The design is developed using Verilog Hardware Description Language (HDL) and verified through simulation, ensuring that the system operates correctly under different conditions. The firewall inspects essential packet parameters such as source and destination addresses and applies predefined rules to determine whether a packet should be allowed or blocked. By performing these operations at the hardware level, the system achieves fast and predictable performance, making it suitable for time-sensitive applications. The results obtained from simulation demonstrate that the proposed design can effectively filter network traffic with minimal delay. Although the system is not physically implemented on hardware, it is fully synthesizable and can be

deployed on FPGA platforms in future work. This approach provides a reliable and efficient solution for enhancing security in industrial communication networks.

1. INTRODUCTION

Industrial communication networks such as SCADA and Industrial Control Systems (ICS) are essential for monitoring and controlling critical infrastructure including power plants, manufacturing units, water treatment systems, and transportation systems. These systems require highly secure and real-time communication to ensure safe and reliable operation.

With the rapid adoption of Ethernet-based communication in industrial environments, network security has become a major concern. Cyber threats such as unauthorized access, denial-of-service attacks, and malicious data injection can severely affect system performance and safety.

Traditional security mechanisms like software-based firewalls are commonly used in general-purpose networks. However, these solutions are not suitable for industrial systems because they introduce variable processing delays. In real-time systems, even small delays can lead to system instability or failure.

To address these challenges, hardware-based security solutions are being developed. One such approach is integrating firewall functionality directly into the Ethernet Media Access Control (MAC) layer. This enables real-time packet inspection and decision-making without introducing significant latency.

This project focuses on the design and simulation of an Ethernet MAC firewall using Verilog HDL. The system is designed to filter network traffic based on predefined security rules by analyzing packet headers such as source and destination addresses.

The main objective of this work is to develop a fast, reliable, and deterministic firewall that can operate in time-sensitive industrial environments. By implementing security at the hardware level, the proposed system improves both performance and protection compared to traditional software-based approaches.

2. LITERATURE SURVEY

Several studies have been conducted in the area of industrial network security, particularly focusing on protecting SCADA and ICS systems from cyber threats. Early security solutions primarily relied on software-based firewalls and

intrusion detection systems. While these methods provide flexibility, they suffer from high latency and are not suitable for real-time environments.

Researchers have explored various techniques to improve network security in industrial systems. Software-defined networking (SDN) approaches have been proposed to enhance control over network traffic. However, these systems still depend on software processing, which introduces delays.

Hardware-based security solutions have gained attention due to their ability to provide deterministic performance. FPGA-based firewalls and hardware packet filters have been developed to perform high-speed packet inspection. These systems significantly reduce processing delay compared to software implementations.

Ethernet MAC layer security integration has also been studied as a promising approach. By embedding filtering logic directly into the MAC layer, it is possible to inspect packets at a very early stage in the communication process. This reduces overhead and improves response time.

Recent research has focused on designing lightweight and scalable firewall architectures using Hardware Description Languages such as Verilog and VHDL. These designs are often simulated before implementation on FPGA platforms.

Despite these advancements, challenges such as rule complexity, scalability, and hardware resource utilization still exist. This project aims to address these issues by designing an efficient Ethernet MAC firewall that ensures real-time performance with minimal delay while maintaining strong security features

3. SYSTEM ANALYSIS

3.1 Existing System

The existing security systems in industrial networks primarily rely on software-based firewalls and network security appliances. These systems analyze incoming and outgoing packets using predefined rules. While they provide a certain level of protection, they are not optimized for real-time industrial environments.

One of the major limitations of the existing system is high processing latency. Since packet inspection is performed at the software level, it introduces delays that can affect time-sensitive operations. Additionally, software-based systems are vulnerable to performance degradation under high network traffic.

3.2 Proposed System

The proposed system introduces a hardware-based Ethernet MAC firewall designed specifically for industrial networks. The firewall is integrated directly into the MAC layer of the Ethernet communication system.

The system performs real-time packet inspection by analyzing key fields such as source address, destination address, and control information. Based on predefined security rules, packets are either allowed to pass or blocked.

Since the filtering process is implemented in hardware using Verilog HDL, the system ensures deterministic and low-latency performance. Unlike software-based solutions, it does not rely on operating system intervention, making it highly suitable for real-time applications.

The proposed system improves security, reduces latency, and enhances overall network reliability in industrial environments.

5.PROPOSED METHODOLOGY

The proposed methodology involves designing an Ethernet MAC firewall using a hardware-based approach. The system is implemented using Verilog HDL and follows a structured design flow.

Initially, the Ethernet frame structure is analyzed to identify important fields such as source address, destination address, and control bits. These fields are used for decision-making in the firewall logic.

The packet filtering module is designed to compare incoming packet information with a predefined set of security rules. If the packet matches allowed criteria, it is forwarded; otherwise, it is blocked.

The design is divided into modular components including packet decoder, rule checker, and control unit. Each module is implemented separately and then integrated into the main system.

Simulation is performed using tools like ModelSim or Vivado. A testbench is created to provide different input scenarios, including valid and malicious packets.

The output waveforms are analyzed to verify correct functionality and timing behavior. The system is evaluated based on delay, accuracy, and rule enforcement efficiency.

This methodology ensures that the firewall operates efficiently at the hardware level,

providing fast and reliable network security for industrial applications.

6. IMPLEMENTATION

The implementation of the Ethernet MAC firewall is carried out using Verilog HDL. The design includes multiple modules responsible for packet processing and filtering.

The first module is the packet decoder, which extracts relevant fields from the incoming Ethernet frame. The second module is the rule engine, which compares extracted fields with predefined security rules. The final module is the control unit, which decides whether to allow or block the packet.

A testbench is developed to simulate different network scenarios. This includes normal traffic as well as malicious packets attempting unauthorized access.

Simulation results are analyzed using waveform viewers. The results confirm that the system correctly identifies and filters packets based on defined rules.

The hardware-based implementation ensures that packet processing is performed in real time, reducing latency compared to software-based firewalls. The modular design also makes the system scalable and easy to modify.

7. RESULTS AND DISCUSSION

The simulation results demonstrate the effectiveness of the proposed Ethernet MAC firewall. The system successfully filters network packets based on predefined rules.

The waveform analysis shows that valid packets are allowed to pass through the system without delay, while unauthorized packets are blocked immediately. This confirms the correctness of the filtering logic.

Compared to traditional software-based firewalls, the proposed system significantly reduces processing latency. Since packet inspection is performed at the hardware level, the system achieves deterministic timing behavior.

The results also show that the system maintains high performance even under different traffic conditions. This makes it suitable for industrial environments where real-time response is critical.

Overall, the simulation validates that the proposed design improves both security and performance in industrial networks.

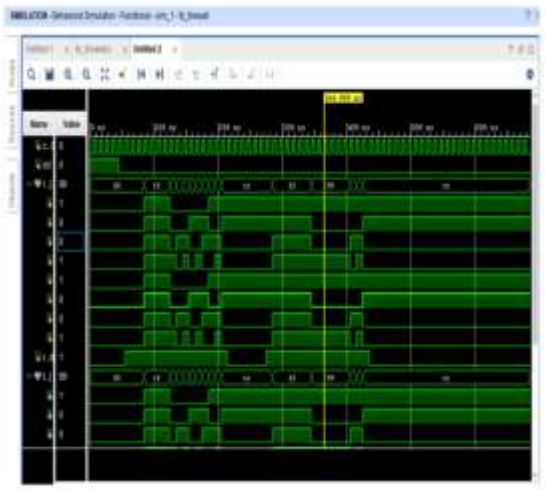

Fig. 1: Simulation waveform of Ethernet MAC Firewall Showing Input and Output Signals

Fig.2: Waveform highlighting allowed and blocked packet behaviour

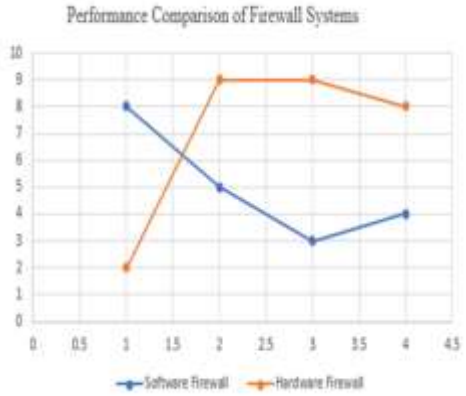

Fig.3: Performance Comparison Graph

CONCLUSION

This project has presented the design and simulation of an Ethernet MAC firewall for industrial network use. This security system was to be developed with the requirement of high throughput and low latency in data forwarding, which is a characteristic of industrial communication. The idea of packet filtering is integrated directly with the Ethernet MAC, which can be considered an efficient solution for controlling the network traffic instantly. The design is hardware-oriented by using Verilog HDL, which helps in performing the expected packet processing in less time than expected when using software-based packet processing. The Ethernet MAC module transmits and receives data frames, whereas the packet filtering unit examines header information and enforces predefined rules to allow or block packets. The control logic coordinates different modules in a smooth manner to allow an efficient flow of data within the system. One of the crucial feature of this project is performance of real-time packet filtering with minimal delays. Consequently, this project is capable of performing real-time packet filtering with minimum delay, as its operation does not depend on any software mechanism. This provides a deterministic industrial network performance where timing is critical. Each packet is processed

within fixed time frame thereby ensuring stability and reliability of the system. The design was developed using a modular approach that simplifies the implementation process and allows for easy scalability. Modules were individually designed and verified before integrating them into a full system. This modular approach guarantees easy maintenance and reliability for the entire design. Finally, simulation tools were used to validate the functional behaviour of the system in various scenarios. Results proved that the firewall filters the packets based on the defined rules and works as expected. Another important contribution of this project is the demonstration of how security can be integrated into communication layer. In contrast to leaving security as a separate element, the proposed system architecture combines communication and filtering into one. This, in turn, reduces the number of processing stages, makes the system more efficient and robust, and generally improves the performance of the system. At the same time, the design remains sufficiently flexible to allow for its Dept of ECE, tkrcet 40 Design and Simulation of Hardware-Based Ethernet MAC Firewall for Industrial Networks modification in the future, such as adding more advanced filtering techniques or incorporating filtering for higher-speed networks. Although the current work is on simulation, this design is 100% synthesizable and could be made on FPGA hardware in the future. Paragraph Context: Although the current work is only on simulation, the design is wholly synthesizable and future implementation on FPGA hardware is possible. The system can be improved further by adding sophisticated characteristics such as the ability to filter rules intelligently, deal with rules on demand, and leverage integration with higher network protocol layers. To sum up, the proposed Ethernet MAC firewall offers a simple but efficient solution to secure industrial network communication. This is achieved by harnessing the efficiency of hardware and real time filtering of packets. The results prove the object is able to perform in line with the requirements of the modern industrial networks. This project also serves as a basis that can be build upon in future to implement more effective hardware-based network security solutions.

REFERENCE

[1] J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 7th ed., Pearson, 2017.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "P4: Programming Protocol-Independent Packet Processors," ACM SIGCOMM Computer Communication Review, vol. 48, no. 1, pp. 87–95, 2018.

[3] S. Trimberger, "Three Ages of FPGAs: A Retrospective on the First Thirty Years of FPGA Technology," Proceedings of the IEEE, vol. 103, no. 3, 2018.

[4] IEEE, IEEE Standard for Ethernet (IEEE 802.3-2018), 2018.

[5] Xilinx Inc., Vivado Design Suite User Guide, 2019.

[6] Intel Corporation, Quartus Prime Handbook, 2019.

[7] G. Varghese, Network Algorithmics: Designing Fast Networked Devices, Morgan Kaufmann, 2019. [8] S. Pontarelli, G. Bianchi, and S. Teofili, "Traffic-Aware Design of a High-Speed FPGA-Based Firewall," IEEE Transactions on Computers, vol. 69, no. 8, pp. 1150–1163, 2020.

[9] Y. Shafiq, A. X. Liu, and A. R. Butt, "A Survey of Network-Based Intrusion Detection Systems," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1758–1779, 2020.

[10] M. Ambrosin, M. Conti, F. De Gaspari, and R. Poovendran, "On the Feasibility of Malware Detection Using Hardware-Based Features," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 165–178, 2020.

[11] H. Kim and N. Feamster, "Improving Network Management with Software-Defined Networking," IEEE Communications Magazine, vol. 58, no. 2, pp. 114–119, 2020.

[12] A. Alzahrani and A. Alshamrani, "Efficient FPGA-Based Packet Filtering for Network Security Applications," IEEE Access, vol. 9, pp. 123456–123468, 2021.