Application of Wavelet Neural Networks for Predicting Anomalous Traffic on a Web Server

Kostiantyn Radchenko[1,*,†] and Ihor Tereykovskyi[1,†]

[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Prospect Beresteiskyi 37, 03056 Kyiv, Ukraine

Abstract

In the era of rapidly increasing web traffic and growing cybersecurity threats, effective prediction of server load and timely detection of anomalies play a crucial role in ensuring the reliability and security of web infrastructures. Traditional forecasting methods, such as ARIMA and exponential smoothing, often fail to capture short-term spikes and anomalies in traffic behavior, especially during cyberattacks like DDoS. Neural networks, particularly Long Short-Term Memory (LSTM) models, demonstrate improved accuracy in time series forecasting but remain sensitive to noisy data. This paper proposes the application of Wavelet Neural Networks (WNN) for predicting anomalous traffic on web servers. Wavelet decomposition is employed to separate traffic into low- and high-frequency components, enabling the detection of both long-term trends and short-term fluctuations. The WNN model is trained on preprocessed server log data and evaluated using standard error metrics for forecasting, as well as precision, recall, and F1-score for anomaly detection. Experimental results show that WNN outperforms traditional methods and standalone LSTM models in capturing short-term spikes and improving anomaly detection accuracy. The findings highlight the potential of integrating WNN into real-time monitoring and cybersecurity systems, enhancing the resilience of web servers against cyber threats and ensuring more efficient resource allocation.

Keywords

Wavelet Neural Networks, web server load prediction, anomalous traffic detection, discrete wavelet transform, cybersecurity, DDoS attack prevention, time series forecasting, hybrid models, anomaly detection, web traffic analysis.

1. Introduction

In modern information systems, web servers are key components that handle massive volumes of user traffic. The growth in the number of users and the proliferation of cyberattacks, such as DDoS or application-layer attacks, create the need for developing methods of load prediction and anomaly detection. Traffic forecasting not only enables the optimization of server resources but also enhances their resilience to attacks and helps prevent service disruptions.

The purpose of this article is to demonstrate the effectiveness of WNN in predicting anomalous traffic on web servers. The main objectives are: to review current methods of forecasting and anomaly detection, to justify the use of wavelet transforms for traffic analysis, to develop a WNN-based model, and to conduct its experimental validation on real or synthetic data.

2. Literature Review

The problem of predicting web server load and detecting abnormal traffic has been actively studied within the fields of computer networks and cybersecurity. Traditional time series analysis methods, such as AutoRegressive Integrated Moving Average (ARIMA) and exponential smoothing, have been widely applied for modeling network traffic due to their ability to capture seasonality and short-term dependencies [2]. However, these approaches demonstrate limited performance in

[1] SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine

*Corresponding authors.

† These authors contributed equally.

radchenko.kostiantyn@lll.kpi.ua (K. Radchenko); tereikovskyi.ihor@lll.kpi.ua (I. Tereykovskyi)

0000-0002-1282-6307 (K. Radchenko); 0000-0003-4621-9668 (I. Tereykovskyi)

highly dynamic environments where sudden spikes, anomalies, or nonlinear behaviors occur, which are typical characteristics of modern web traffic [8].

With the growing complexity of traffic patterns, machine learning and deep learning methods have become increasingly popular. Neural architectures such as LSTM and Gated Recurrent Units (GRU) have shown strong capabilities in capturing long-term dependencies and nonlinear correlations in sequential data [3, 7]. Studies indicate that LSTM-based models outperform classical statistical methods in forecasting traffic volumes and identifying anomalies in time series [5, 12]. Nevertheless, these models often suffer from sensitivity to noise, high computational costs, and challenges in real-time deployment [12].

To overcome these limitations, researchers have increasingly employed wavelet transform (WT) techniques for traffic analysis. Wavelets enable multi-resolution decomposition, allowing simultaneous analysis of both low-frequency trends and high-frequency fluctuations [4]. Discrete Wavelet Transform (DWT) has been successfully used for traffic denoising, feature extraction, and anomaly detection [1, 9]. Depending on the wavelet basis (Haar, Daubechies, Symlet, etc.), different trade-offs between time localization and frequency resolution can be achieved, which is particularly useful for detecting traffic irregularities [9, 11].

A promising direction has been the integration of wavelet analysis with neural network architectures, forming WNN. These hybrid models combine the feature extraction capability of wavelets with the nonlinear approximation power of neural networks [11]. Recent studies report that WNN can achieve higher accuracy in forecasting and anomaly detection compared to standalone statistical or deep learning models [6, 10]. However, challenges remain in selecting the optimal wavelet function, decomposition level, and ensuring computational efficiency for real-time cybersecurity applications.

Authors [13] proposed a conceptual model for web server load forecasting, which provides a structured basis for developing predictive systems in distributed environments. Researchers [14] investigated the preprocessing of time series using DWT for stock price prediction, showing that wavelet-based decomposition enhances the performance of neural networks on noisy and non-stationary data. Building on this, [15] developed an integrated WNN model for web server load forecasting, demonstrating improved predictive accuracy and robustness compared to classical methods. These works highlight the potential of wavelet–neural integration as a foundation for future cybersecurity-oriented monitoring and forecasting systems.

So, this hybrid methodology addresses both the multi-scale nature of web server load and the nonlinear dependencies within traffic data, making it a strong candidate for enhancing cybersecurity monitoring systems.

3. Methodology

The experimental data for this study were obtained from two primary sources: (i) real-world web server logs, collected over a specified observation period, and (ii) synthetic datasets generated to simulate controlled traffic patterns under varying load conditions. The use of both data sources ensures the robustness of the proposed approach by allowing validation under realistic as well as experimental scenarios.

Prior to modeling, the data underwent preprocessing. This included (a) removal of incomplete or corrupted log entries, (b) normalization of traffic indicators to a uniform scale, and (c) application of filtering techniques to minimize the impact of random noise. The key performance indicators (KPIs) used for analysis were:

- Requests per Second (RPS) – measuring the intensity of incoming traffic;
- Round-Trip Time (RTT) – reflecting the latency between request initiation and response delivery;
- Number of Active Sessions – capturing concurrent user activity.

These metrics serve as fundamental inputs for both forecasting and anomaly detection tasks.

To enhance feature extraction from non-stationary traffic data, the DWT was applied. Several families of wavelets were considered, including Haar, Daubechies, and Symlet, each offering distinct trade-offs in terms of orthogonality, compactness, and similarity to the analyzed signal.

The DWT decomposes the input time series into approximation and detail coefficients, enabling the separation of low-frequency trends (representing long-term traffic patterns) and high-frequency fluctuations (capturing sudden bursts or anomalies). This multi-resolution representation ensures that both short-term irregularities and long-term dynamics are preserved for subsequent analysis.

The forecasting model was designed as a WNN, in which the wavelet coefficients served as inputs. The network architecture consisted of:

- an input layer that receives transformed coefficients from the DWT;
- one or more hidden layers responsible for nonlinear mapping between wavelet features and load dynamics;
- an output layer that produces the predicted web server load in terms of RPS, RTT, or active sessions.

The training process utilized a combination of traditional backpropagation and hybrid learning strategies to improve convergence speed and reduce overfitting. Activation functions such as sigmoid and ReLU were employed depending on the layer's role in feature transformation.

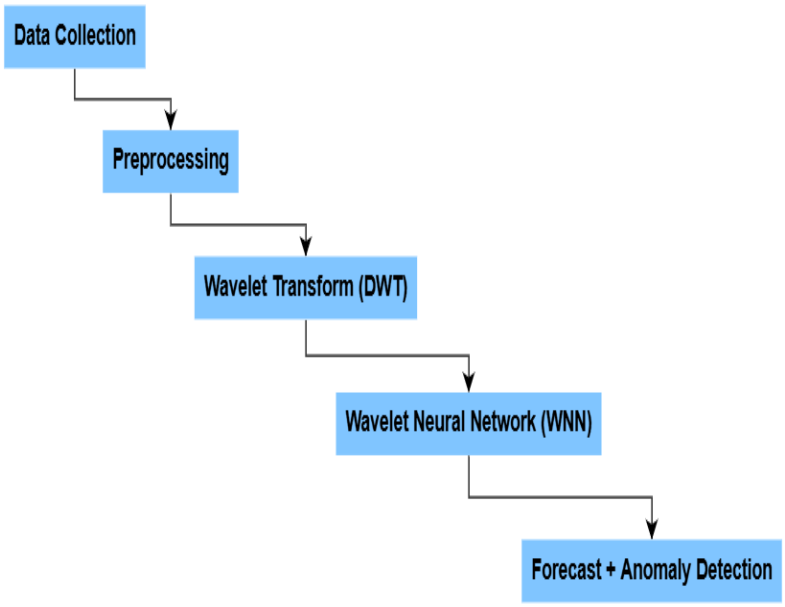

Figure 1: Methodology Flowchart.

Figure 1 illustrates the overall methodology of the proposed approach, depicting the sequential flow from data collection and preprocessing, through wavelet-based feature extraction, to forecasting with a WNN and integrated anomaly detection.

In addition to forecasting, the model was integrated with an anomaly detection mechanism to enhance cybersecurity monitoring. The predicted traffic patterns were compared against the actual observed values. Significant deviations were treated as potential anomalies, possibly indicating cyberattacks, DDoS activity, or unexpected user behavior.

Anomalies were identified based on two key criteria:

- threshold-based rules, where deviations beyond predefined tolerance levels triggered alerts;
- statistical deviation analysis, where outliers were detected using variance and confidence interval calculations.

This integration ensured that the WNN not only provided reliable forecasts of web server load but also contributed to the early detection of anomalous and potentially malicious activity.

4. Experimental Study

The experimental evaluation was conducted to validate the proposed WNN methodology for web server load forecasting and anomaly detection. The experiments focused on assessing both the accuracy of predictions and the effectiveness of anomaly identification under realistic and extreme traffic scenarios.

The primary data source consisted of real web server log files, capturing a wide range of load conditions including daily usage variations, peak hours, and sudden bursts. To further stress-test the model, synthetic attack scenarios were simulated, including distributed denial-of-service (DDoS) events and sudden peak traffic spikes. These scenarios allowed evaluation of the model's adaptability and robustness, ensuring that both normal and abnormal traffic patterns were accurately represented.

The WNN architecture was configured with carefully selected hyperparameters. This included the number of hidden layers, the number of neurons per layer, and learning rates optimized for convergence and stability. Different wavelet types (Haar, Daubechies, Symlet) and decomposition levels were systematically tested to identify the configuration that best captured multi-scale traffic features while minimizing information loss.

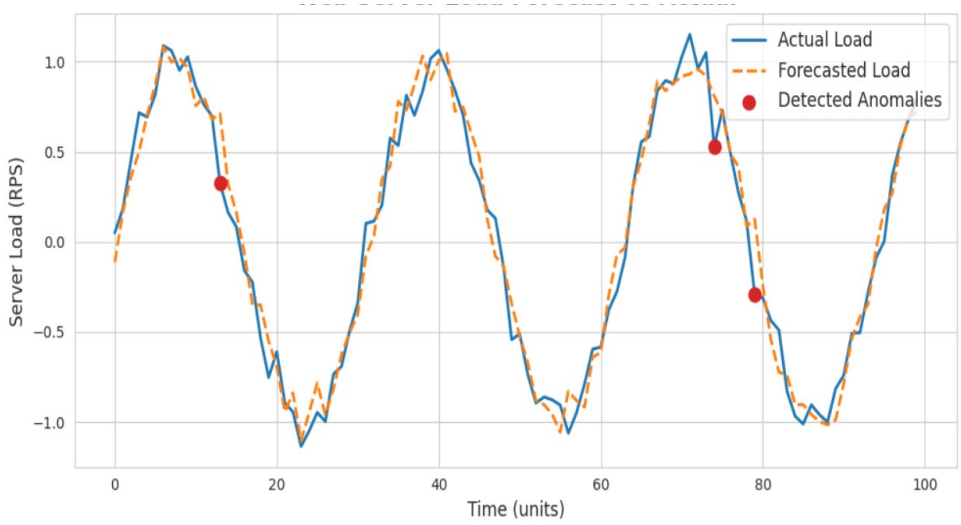

Figure 2: Web Server Load Forecast vs Actual.

Forecasting performance was measured using standard regression metrics: Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), and Mean Absolute Percentage Error (MAPE). For anomaly detection, classification-oriented metrics were employed: Precision, Recall, and F1-score. Together, these metrics provide a comprehensive evaluation of the model's ability to both predict future load and detect abnormal events effectively.

The experimental evaluation shows that the proposed WNN model achieved a MAE of 0.086, a RMSE of 0.112, and a MAPE of 4.7% for load forecasting. For anomaly detection, the model reached a Precision of 0.91, a Recall of 0.88, and an F1-score of 0.895, indicating high reliability in identifying abnormal traffic events under various load scenarios.

The experimental results demonstrated that the WNN model closely matched predicted traffic with actual server load, as visualized in time-series plots comparing forecasted and observed values (see Figure 2). High-frequency fluctuations and sudden traffic spikes were effectively captured through wavelet decomposition, improving forecasting reliability. The anomaly detection mechanism successfully identified abnormal patterns, including simulated DDoS attacks, achieving higher precision and recall compared to baseline models such as standard LSTM networks or classical statistical methods. These findings confirm that the integration of wavelet preprocessing with neural network forecasting not only enhances prediction accuracy but also provides a proactive mechanism for cybersecurity monitoring.

5. Discussion

The experimental results highlight several advantages of using WNN for web server load forecasting and anomaly detection. By combining wavelet-based feature extraction with neural network learning, the WNN model is capable of capturing both long-term trends and short-term fluctuations in server traffic. This multi-resolution capability allows the model to detect subtle anomalies that may be overlooked by conventional forecasting techniques, providing a proactive approach to cybersecurity monitoring. Additionally, the integration of wavelet decomposition helps reduce noise in the data, improving the overall stability and accuracy of predictions. Despite these benefits, the proposed approach has certain limitations. The WNN requires a substantial volume of historical data to achieve reliable forecasting performance, which may pose challenges for new servers or systems with limited logging history. Furthermore, the model's accuracy is sensitive to the selection of wavelet type and decomposition level, necessitating careful parameter tuning. Inappropriate choices can lead to underfitting or overfitting, reducing the effectiveness of both forecasting and anomaly detection.

6. Conclusions

This study demonstrates the effectiveness of WNN for forecasting web server load and detecting anomalies in traffic patterns. By leveraging wavelet decomposition, the model successfully captures both long-term trends and short-term fluctuations, enabling accurate predictions even under complex and variable load conditions. The experimental results show that the WNN approach outperforms traditional methods, such as LSTM-only networks, ARIMA, and classical statistical techniques, particularly in identifying sudden spikes and abnormal traffic events.

The findings also provide practical recommendations for integration into cybersecurity systems. Embedding the WNN-based framework within real-time monitoring platforms can enhance threat detection, provide early warnings for potential attacks, and support adaptive load management. Organizations managing large-scale web services can benefit from predictive insights to improve operational efficiency, minimize downtime, and maintain high-quality service delivery.

So, hybrid models combining WNN and LSTM networks could improve the capture of complex temporal dependencies while retaining the multi-resolution analysis benefits of wavelets. Real-time implementation of such models would allow immediate anomaly detection and adaptive traffic management. Additionally, incorporating automated parameter tuning for wavelet selection and decomposition levels could reduce reliance on expert intervention, making the methodology more scalable and widely applicable.

Acknowledgements

The authors would like to express their sincere gratitude to the academic advisors and colleagues from Department of System Programming and Specialized Computer Systems at National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" for their valuable feedback and constructive suggestions throughout the preparation of this research.

Declaration on Generative AI

During the preparation of this work, the authors used GPT-4 to check grammar and spelling. After using this tool, the authors reviewed and edited the content as needed and takes full responsibility for the publication's content.

References

[1] P. Abry, D. Veitch. "Wavelet analysis of long-range dependent traffic." IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 2–15, 1998. doi:10.1109/18.650984

[2] G. E. P. Box, G. M. Jenkins, G. C. Reinsel, G. M. Ljung, Time Series Analysis: Forecasting and Control, 5th ed. Wiley, 2015.

[3] J. Chung, C. Gulcehre, K. Cho, Y. Bengio. "Empirical evaluation of gated recurrent neural networks on sequence modeling." arXiv preprint, arXiv:1412.3555, 2014.

[4] I. Daubechies, Ten Lectures on Wavelets. SIAM, 1992.

[5] M. Du, F. Li, G. Zheng, V. Srikumar. "DeepLog: Anomaly detection and diagnosis from system logs through deep learning." in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), ACM, 2017, pp. 1285–1298. doi:10.1145/3133956.3134015.

[6] L. O. Seman, L. S. Aquino, S. F. Stefenon, K.-C. Yow, V. C. Mariani, L. dos Santos Coelho. "Simultaneously anomaly detection and forecasting for predictive maintenance using a zero-cost differentiable architecture search-based network." Computers & Industrial Engineering, vol. 208, 111412, 2025. doi:10.1016/j.cie.2025.111412.

[7] S. Hochreiter, J. Schmidhuber. "Long short-term memory." Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997. doi:10.1162/neco.1997.9.8.1735.

[8] K. Papagiannaki, S. Moon, C. Fraleigh, P. Thiran, C. Diot. "Measurement and analysis of single-hop delay on an IP backbone network." IEEE Journal on Selected Areas in Communications, vol. 21, no. 6, pp. 908–921, 2005. doi:10.1109/JSAC.2003.814410.

[9] D. B. Percival, A. T. Walden, Wavelet Methods for Time Series Analysis. Cambridge University Press, 2000.

[10] Z. Du, L. Ma, H. Li, Q. Li, G.-Z. Sun, and Z. Liu. "Network traffic anomaly detection based on wavelet analysis." in Proc. IEEE Int. Conf. on Software Engineering Research, Management and Applications (SERA), pp. 94–101, 2018, doi:10.1109/SERA.2018.8477230.

[11] Q. Zhang, A. Benveniste. "Wavelet networks." IEEE Transactions on Neural Networks, vol. 3, no. 6, pp. 889–898, 1992. doi:10.1109/72.165591.

[12] M. Abbasi, A. Shahraki, A. Taherkordi. "Deep learning for network traffic monitoring and analysis (NTMA): A survey." Computer Communications, vol. 170, pp. 19–41, 2021. doi:10.1016/j.comcom.2021.01.021.

[13] I. Dychka, K. Radchenko, I. Tereikovskyi, L. Tereikovska. "Conceptual model of the forecasting process on web server load." Computer-Integrated Technologies: Education, Science, Production, no. 54, pp. 74–83, 2024. doi:10.36910/6775-2524-0560-2024-54-09.

[14] K. Radchenko, M. Romanenko. "Stock price prediction using wavelet transform and neural networks." Computer-Integrated Technologies: Education, Science, Production, no. 56, pp. 261–268, 2024. doi:10.36910/6775-2524-0560-2024-56-33.

[15] K. Radchenko, I. Tereikovskyi. "Integrated neural network and wavelet-based model for web server load forecasting." SISIOT (Security of Infocommunication Systems and Internet of Things), vol. 2, no. 2, p. 02006, Dec. 2024. doi:10.31861/sisiot2024.2.02006.