A Dual-Objective CART Model for Throughput Estimation and Real-Time Malicious Activity Detection in 6G Networks

Teegala Supraja[1], Karramareddy Sharmila[2*], T. Sushma[3]

[1]PG Student, [2]Associate Professor and Head, [3]Assistant Professor, [1,2,3]Department of Computer Science and Engineering
[1,2,3]Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
[1]teegalasupraja2002@gmail.com
*Correspondence: Karramareddy Sharmila (sharmilakreddy@gmail.com)

ABSTRACT

The emergence of sixth generation (6G) communication networks has created a growing need for intelligent, secure, and high-performance network management solutions capable of handling increasingly complex communication environments. Conventional network monitoring and intrusion detection systems largely depend on manual analysis and administrator expertise, which limits their effectiveness in large-scale and dynamic network infrastructures. These traditional approaches are often time-intensive, susceptible to human error, and inadequate for identifying sophisticated cyberattacks while maintaining optimal network performance. To address these challenges, this study presents a hybrid machine learning-based framework for simultaneous attack classification and throughput prediction. The proposed methodology incorporates comprehensive data preprocessing techniques, including Label Encoding for categorical feature transformation, Standardization for feature normalization, and Synthetic Minority Over-sampling Technique (SMOTE) for class imbalance mitigation. Initially, deep discriminative features are extracted from network traffic data to capture complex behavioral patterns. These features are subsequently processed using the proposed Graph Neural Network-based Sparse Linear Interpretable Model (GNN-SLIM), which performs both classification and regression tasks. To evaluate the effectiveness of the proposed approach, its performance is compared against several benchmark models, including Support Vector Machine (SVM), k-Nearest Neighbors (KNN), and Tree Alternative Optimization (TAO) Tree algorithms. The integration of graph-based learning and interpretable modeling enhances feature representation, improves generalization capability, and increases robustness under diverse network conditions. Experimental findings demonstrate that the proposed GNN-SLIM framework achieves higher attack detection accuracy and more reliable throughput prediction than the comparative models. Additionally, a Flask-based web application is developed to facilitate real-time network analysis and interactive user access. The proposed framework offers a scalable, intelligent, and efficient solution for enhancing cybersecurity and communication performance in next generation 6G network environments.

Key words: 6G communication networks, Graph Neural Networks (GNN), intrusion detection systems, machine learning, throughput prediction.

1.INTRODUCTION

Network management and monitoring systems rely on standardized data collection protocols such as Simple Network Management Protocol (SNMP), NetFlow, Internet Protocol Flow Information Export (IPFIX), and Network Configuration Protocol (NETCONF) [1]. Organizations often develop customized monitoring solutions based on these protocols to obtain comprehensive visibility into network operations and to effectively identify

Doi:10.48047/ijiee.2026.16.2.49

performance degradation, faults, and security-related issues. With the continuous expansion of communication services and applications, the complexity and scale of network infrastructures have increased substantially. Consequently, modern network devices generate enormous volumes of data, including control messages, statistical information, configuration records, and user traffic, at an unprecedented rate [2].

The analysis of such large-scale and heterogeneous datasets using conventional manual or semi-automated approaches requires significant technical expertise, processing time, and operational resources. As network environments continue to evolve in complexity, these traditional methods become increasingly inefficient and difficult to maintain. This situation has accelerated the adoption of intelligent and automated analytical solutions capable of processing high-dimensional data and supporting rapid, accurate decision-making within modern communication infrastructures.

One of the most significant technological advancements facilitating intelligent network management is Software-Defined Networking (SDN) [3]. SDN introduces a centralized and programmable control architecture that enhances network flexibility, simplifies configuration management, and improves resource utilization. Despite these advantages, SDN environments still require continuous monitoring and efficient anomaly detection mechanisms to maintain security and operational stability. The centralized collection of network data enables improved aggregation, coordination, and correlation of information across multiple network components. However, the storage, processing, and analysis of such massive datasets create substantial computational challenges commonly associated with big data analytics [4].

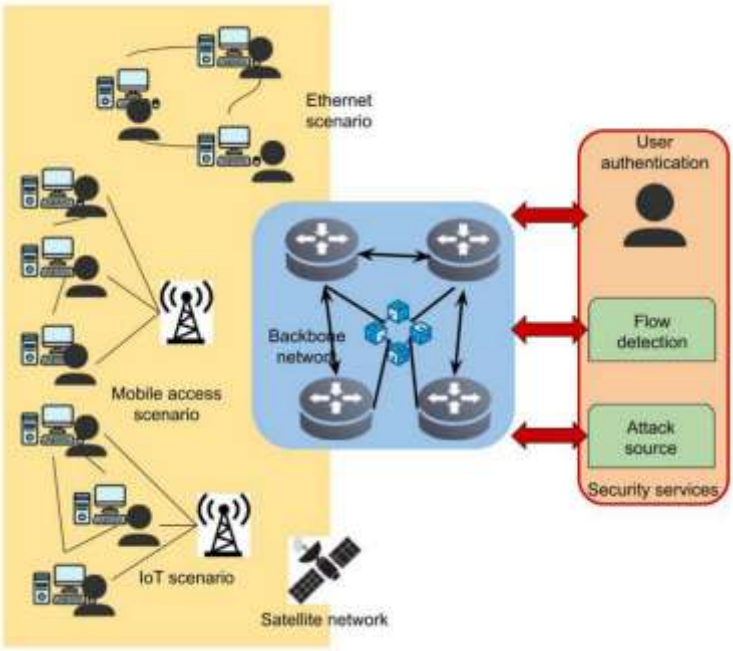


Figure 1. Architecture for Heterogeneous 6G Network Environments.

Figure 1 illustrates a comprehensive security architecture for a heterogeneous 6G network that integrates multiple access scenarios, including Ethernet networks, mobile communication networks, IoT environments, and satellite communications through a unified backbone network. The backbone network interconnects diverse users, devices, and communication infrastructures while enabling seamless data exchange across different domains. To address

Doi:10.48047/ijiee.2026.16.2.49

emerging 6G security challenges, dedicated security services are integrated with the backbone network, comprising user authentication, flow detection, and attack source identification modules. The user authentication component ensures that only legitimate users and devices gain network access, preventing unauthorized entry and identity-based attacks.

The flow detection module continuously monitors network traffic to identify abnormal communication patterns, malicious flows, and distributed cyber threats in real time. The attack source identification mechanism traces the origin of detected attacks, enabling rapid mitigation and response actions. By combining these security functions across terrestrial, mobile, IoT, and satellite communication environments, the proposed architecture enhances confidentiality, integrity, availability, and trustworthiness, making it suitable for securing highly dynamic and large-scale 6G networks against sophisticated cyberattacks.

1.2 Research Objective

- To develop a hybrid framework for intelligent intrusion detection and network throughput prediction in 6G communication networks using CART-based learning.
- To implement and compare SVM, KNN, TAO Tree, and the proposed GNN-SLIM model for accurate detection and classification of malicious network activities.
- To design an integrated regression model for predicting network throughput, enabling simultaneous analysis of network performance and network security.

2. LITERATURE SURVEY

Braeken et al. [5] proposed a comprehensive AI-driven security framework for 6G networks by examining the security implications of AI-native communication architectures. The authors analyzed offensive and defensive AI mechanisms across infrastructure, network service, and application layers. They categorized AI-enabled cyber threats and mapped them to corresponding mitigation techniques. The study further evaluated multiple security frameworks and explored the integration of quantum-enhanced security mechanisms for resilient 6G environments. Additionally, open research challenges and future security requirements were systematically identified for trustworthy AI-enabled 6G systems. The work mainly provides a survey-based analysis and lacks practical implementation and performance validation in real-world 6G deployments. Shaji et al. [6] developed a machine learning-based physical layer security model for 5G/6G-enabled electric vehicle charging networks. The methodology utilized wireless channel characteristics and intelligent learning algorithms to identify abnormal communication behavior. Feature extraction was performed from physical layer parameters to distinguish legitimate and malicious users. The model employed supervised learning techniques for attack detection and authentication enhancement. Security performance was evaluated under different charging network scenarios to improve communication reliability and privacy. The framework primarily focuses on physical layer attacks and does not address higher-layer security threats comprehensively.

Altintaş et al. [7] introduced a detailed investigation of adversarial threats targeting AI-native 6G systems. The authors analyzed different attack models including evasion, poisoning, model extraction, and inference attacks. A taxonomy of adversarial machine learning threats was developed for future intelligent communication networks. The study evaluated vulnerabilities of AI models embedded in 6G architectures and discussed defensive mechanisms against adversarial manipulation. Furthermore, mitigation strategies based on robust learning and trustworthy AI principles were presented. The proposed defenses incur additional computational overhead, which may affect resource-constrained 6G devices. Alwaisi

Doi:10.48047/ijiee.2026.16.2.49

and Soderi [8] implemented a semantic communication-based framework for detecting False Data Injection Attacks in 6G-enabled smart grids. The approach leveraged semantic information extraction to analyze transmitted data beyond conventional bit-level communication. Machine learning techniques were integrated to identify malicious alterations in smart grid measurements. The framework evaluated communication efficiency and attack detection accuracy simultaneously. The model depends heavily on semantic feature quality, which may degrade under dynamic network conditions.

De Alwis et al. [9] presented a federated learning-based security architecture for 6G networks. The methodology investigated distributed model training without sharing raw user data, thereby preserving privacy. Various federated learning threats including poisoning, inference, and backdoor attacks were analyzed. Countermeasures such as secure aggregation, differential privacy, and robust model updating were evaluated. The framework also identified future research directions for secure collaborative learning in 6G ecosystems. Communication overhead and model synchronization complexity remain significant challenges in large-scale deployments. Alwaisi et al. [10] developed an energy-aware intrusion detection mechanism for identifying Mirai botnet attacks in 6G-enabled IoT networks. The methodology combined lightweight traffic analysis with intelligent classification techniques. Network behavioral features were extracted to differentiate botnet traffic from legitimate communication. Energy-efficient detection strategies were incorporated to support resource-limited IoT devices. PDetection accuracy may decrease when facing previously unseen botnet variants.

Tripathi et al. [11] proposed an adversarial machine learning framework to enhance cybersecurity resilience in 6G networks. The methodology integrated adversarial training techniques to improve the robustness of AI-based security models. Attack simulations were performed to evaluate the vulnerability of learning algorithms. Defensive strategies were designed to withstand sophisticated adversarial manipulations. The framework strengthened the adaptability of security systems against evolving cyber threats. Adversarial training significantly increases computational complexity and training time. Harsora et al. [12] conducted a comprehensive study on 6G technologies, security challenges, and potential cyberattacks. The methodology classified emerging threats associated with AI, blockchain, edge computing, and network virtualization. Various attack surfaces within future communication architectures were systematically examined. Security requirements and defense mechanisms were reviewed across multiple networking layers. Future research opportunities were also highlighted to improve network resilience. The work remains theoretical and does not provide experimental validation of the discussed solutions.

Kulkarni et al. [13] introduced a blockchain-based cybersecurity framework for 5G/6G Industrial IoT applications. The methodology integrated blockchain technology with neural networks and graph learning models for secure data exchange. Smart contracts were utilized to automate trust management and authentication processes. Graph-based intelligence enhanced anomaly detection capabilities within industrial and healthcare environments. The framework improved transparency, decentralization, and security across connected devices. Blockchain integration introduces latency and increased storage requirements. Vivekanandan et al. [14] implemented a cloud-based intrusion detection framework utilizing BSO-ResNet for malicious packet detection in 6G networks. The approach combined Beetle Swarm Optimization with deep residual networks for feature optimization and classification. Cloud computing resources were

Doi:10.48047/ijiee.2026.16.2.49

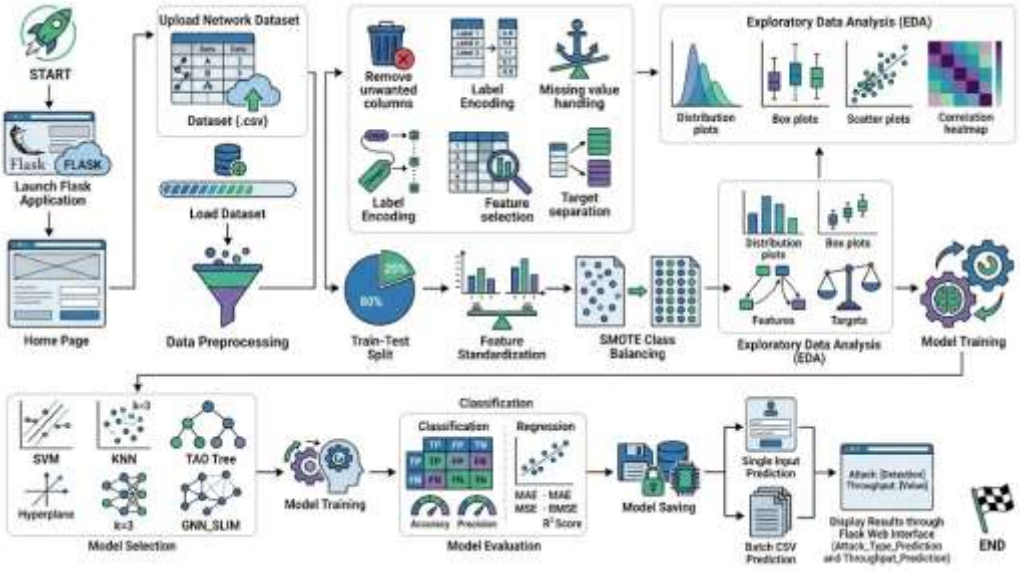
employed to handle large-scale network traffic. Anegdouil et al. [15] developed a transformer-based web attack detection system for 6G MEC-enabled SDN architectures. The methodology employed transformer networks to capture complex traffic patterns and attack signatures. Edge computing resources were utilized for real-time analysis and response. SDN controllers facilitated dynamic traffic monitoring and policy enforcement.

3. PROPOSED METHODOLOGY

The proposed framework is designed to provide an intelligent and automated solution for simultaneous network attack detection and throughput prediction in 6G communication environments. The workflow begins with uploading the network dataset through a Flask-based web interface, followed by comprehensive preprocessing to improve data quality and consistency. After preprocessing, the dataset undergoes exploratory data analysis to identify important statistical characteristics and feature relationships. Subsequently, the processed data are divided into training and testing sets, standardized, and balanced using SMOTE before being supplied to the selected machine learning models. The framework incorporates SVM, KNN, TAO Tree, and the proposed GNN-SLIM model for comparative analysis and predictive learning. During evaluation, both classification and regression performance are measured using multiple performance metrics, after which the trained models are saved for future use. Figure 2 illustrates the complete workflow of the proposed framework, beginning from dataset acquisition and preprocessing through model training, evaluation, and real-time prediction using the Flask-based application. The architecture enables efficient attack classification and throughput prediction, thereby improving network security and communication performance in next generation 6G networks.

Step 1: Dataset Acquisition and Preprocessing

The framework begins by uploading the network dataset through the Flask-based application. The uploaded dataset is loaded into the system, where unnecessary columns are removed, categorical attributes are encoded, missing values are handled, and the feature and target variables are separated. These preprocessing operations improve data quality, eliminate inconsistencies, and prepare the dataset for effective machine learning.



Doi:10.48047/ijiee.2026.16.2.49

Figure 2: Proposed system architecture for real-time malicious activity detection in 6G networks

Step 2: Data Preparation and Exploratory Data Analysis

The processed dataset is divided into training and testing subsets using an 80:20 ratio. Feature values are standardized to maintain uniform scaling, while SMOTE is applied to balance the class distribution and minimize prediction bias. Exploratory Data Analysis (EDA) is then performed to examine feature distributions, target distributions, statistical relationships, and correlations within the dataset.

Step 3: Model Selection and Training

The prepared dataset is supplied to the selected machine learning models, including SVM, KNN, TAO Tree, and the proposed GNN-SLIM framework. Each model learns the underlying characteristics of network traffic to perform attack classification and throughput prediction simultaneously. The training process enables the framework to capture complex traffic patterns and generate robust predictive models.

Step 4: Performance Evaluation and Model Storage

The trained models are evaluated using classification metrics such as Accuracy, Precision, Recall, and F1-Score, along with regression metrics including MAE, MSE, RMSE, and R^2 Score. The evaluation results are analyzed to compare the performance of different models. Subsequently, the trained models are stored to facilitate future predictions without requiring retraining.

Step 5: Real-Time Prediction and Result Visualization

The saved models are utilized to perform predictions on both single-user inputs and uploaded batch datasets. The framework simultaneously predicts the network attack category and throughput value, and the generated results are displayed through the Flask web interface. This real-time prediction capability enables efficient monitoring, analysis, and decision-making for secure and optimized 6G communication networks.

4. RESULTS AND DISCUSSION

The implementation of the system is designed as a fully integrated web-based machine learning application that performs simultaneous attack classification and throughput prediction using the proposed GNN-SLIM framework together with the existing SVM, KNN, and TAO Tree models. The system follows a modular pipeline architecture, enabling efficient data preprocessing, feature learning, model training, evaluation, model storage, and real-time prediction through a Flask-based web application.

Figure 3 Exploratory data analysis of network data. countplot of attack types (toprow-left). Boxplot of latency distribution per attack type (toprow - middle). Voilin plot of signal strength by attack type (toprow-right). Boxplot of throughput by signal strength (bottom row - left). Scatter plot of throughput vs latency (bottom row - middle). Correlation heatmap with throughput (bottom row - right).

Fig a: Distribution of Attack Types

This bar chart displays the distribution of three attack types (encoded as 0, 1, and 2) based on their count. The x-axis represents the attack types, and the y-axis shows the count. The bars indicate that each attack type has a different frequency, with attack type 0 having the highest count, followed by type 2, and type 1 having the lowest.

Fig b: Latency Distribution per Attack Type

This box plot illustrates the latency distribution (in milliseconds) for the three attack types (encoded as 0, 1, and 2). The x-axis represents the attack types, and the y-axis shows the latency. The boxes and whiskers provide a summary of the median, quartiles, and range of latency values for each attack type, showing variations in latency across the types.

Fig c: Signal Strength by Attack Type

Doi:10.48047/ijiee.2026.16.2.49

This violin plot depicts the signal strength (encoded values) for the three attack types (encoded as 0, 1, and 2). The x-axis represents the attack types, and the y-axis shows the signal strength. The width of each violin indicates the density of data points, highlighting the distribution and central tendency of signal strength for each attack type.

.

Fig d: Throughput by Signal Strength

This box plot shows the throughput (in Mbps) across different signal strength levels (encoded as 0, 1, and 2). The x-axis represents signal strength, and the y-axis shows throughput. The boxes and whiskers summarize the median, quartiles, and range of throughput values, indicating how throughput varies with signal strength

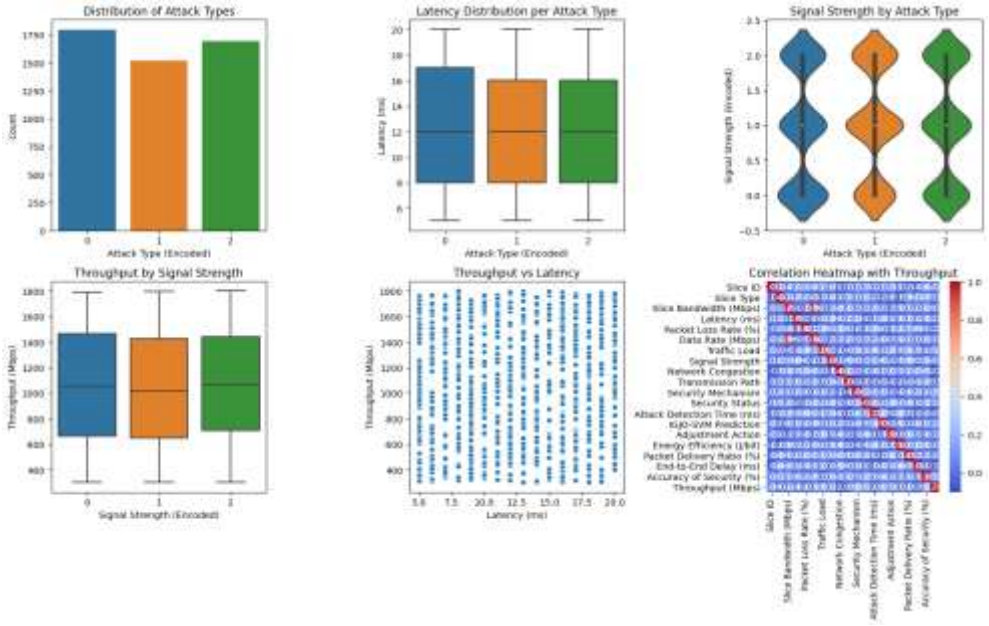


Figure 3: Data Analysis of Network Dataset. (a), (b), (c), (d), (e), (f).

Fig e: Throughput vs Latency

This scatter plot examines the relationship between throughput (in Mbps) and latency (in milliseconds). The x-axis represents latency, and the y-axis represents throughput. The scattered points suggest a pattern or correlation between these two metrics, with a higher density of points around certain latency and throughput combinations.

Fig f: Correlation Heatmap with Throughput

This heatmap displays the correlation coefficients between throughput and various other metrics (e.g., Slice ID, Slice Bandwidth, Packet Loss Rate). The x-axis and y-axis list the metrics, with color intensity (from blue to red) indicating the strength and direction of the correlation, ranging from -1 to 1. Stronger correlations are shown in warmer colours.

The scatter plots in Figure 4 compare the actual and predicted throughput values for four models: GNN-SLIM. The SVM plot shows a flat predicted value trend, indicating poor performance. The KNN plot shows predictions closely aligned with the diagonal, suggesting good accuracy. The TAO Tree Regressor exhibits improved prediction capability with a stronger correlation between actual and predicted throughput values. The proposed GNN-SLIM model demonstrates the highest regression performance, with most prediction points concentrated very close to the ideal diagonal line, indicating excellent agreement between actual

Doi:10.48047/ijiee.2026.16.2.49

and predicted throughput values. Although a few samples exhibit minor deviations, the overall distribution confirms that GNN-SLIM achieves highly accurate throughput estimation with lower prediction error and better generalization compared to the existing models.

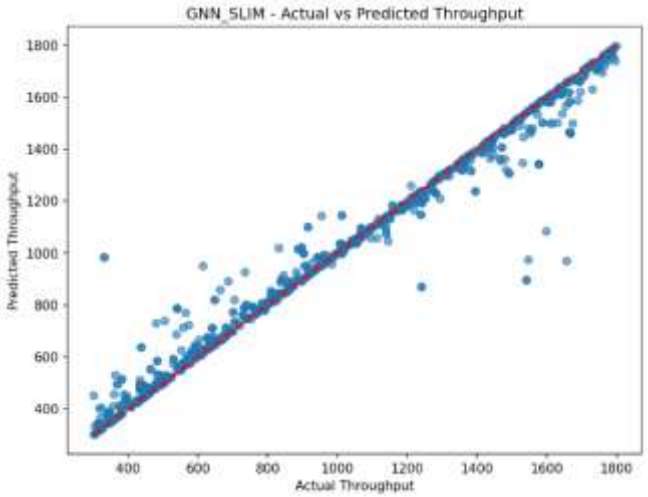


Figure 4: Scatter plot of actual vs predictions obtained using GNN-SLIM Regressor

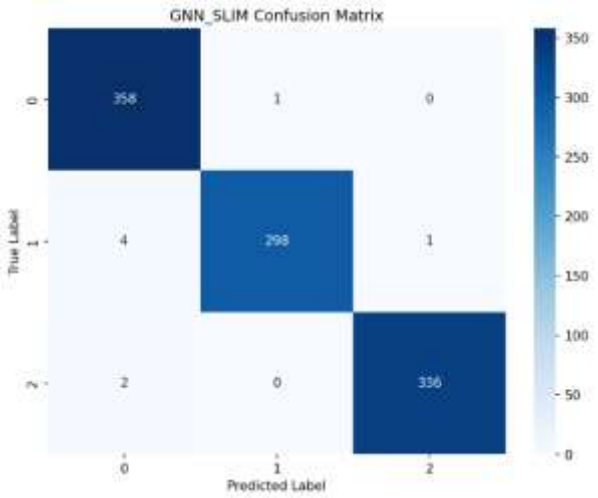


Figure 5: Confusion matrix obtained using GNN-SLIM Classifier

The confusion matrices in Figure 5 illustrate the performance of four models: GNN-SLIM in classifying DDoS, Eavesdropping, and Spoofing attacks. Table 1 presents the regression performance comparison of the implemented models using MAE, MSE, RMSE, and R^2 Score. The SVR model exhibits the poorest performance with the highest prediction errors and a very low R^2 Score of 0.009, indicating weak regression capability. The KNN model significantly improves the prediction accuracy, reducing the overall error and achieving an R^2 Score of 0.739.

Doi:10.48047/ijiee.2026.16.2.49

The TAO Tree Regressor further enhances the prediction performance with lower error values and an R^2 Score of 0.969. The proposed GNN-SLIM framework achieves the best overall regression performance, producing the lowest MSE (5444.718), the lowest RMSE (73.788), and the highest R^2 Score (0.971), while maintaining a low MAE of 28.391. These results demonstrate that GNN-SLIM provides more accurate and reliable throughput prediction than the existing regression models, making it the most effective framework for network performance estimation.

Table 1: Performance evaluation obtained using existing SVM, KNN regressors, TAO Tree and GNN-SLIM regression models.

Model	**MAE**	**MSE**	**RMSE**	**R^2 Score**
SVR Model	370.871	186,609.000	431.828	0.009
KNN Model	133.998	49,133.987	221.662	0.739
TAO Tree Regressor	0.0297	5,787.744	76.007	0.969
GNN-SLIM	**28.391**	**5,444.718**	**73.788**	**0.971**

Table 2: Performance evaluation obtained using existing SVM, LR, KNN, TAO Tree and GNN-SLIM classification models.

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**
SVC Model	89.70%	89.70%	89.70%	89.70%
KNN Model	88.90%	88.907%	88.850%	88.876%
TAO Tree Classifier	98.70%	98.70%	98.70%	98.70%
GNN-SLIM (Proposed)	**99.92%**	**99.92%**	**99.92%**	**99.92%**

Table 2 presents the classification performance comparison of the implemented models using Accuracy, Precision, Recall, and F1-Score. The SVC model achieves an overall accuracy of 89.70%, demonstrating moderate classification performance across the attack categories. The KNN model provides comparable results with an accuracy of 88.90% and similar Precision, Recall, and F1-Score values. The TAO Tree Classifier significantly improves the classification performance by achieving 98.70% across all evaluation metrics, indicating its effectiveness in distinguishing different network attacks. The proposed GNN-SLIM framework outperforms all existing models by achieving 99.92% for Accuracy, Precision, Recall, and F1-Score. These results confirm that the proposed framework provides highly reliable attack classification with minimal misclassification, making it the most effective model for intelligent network intrusion detection in 6G communication environments.

Doi:10.48047/ijiee.2026.16.2.49

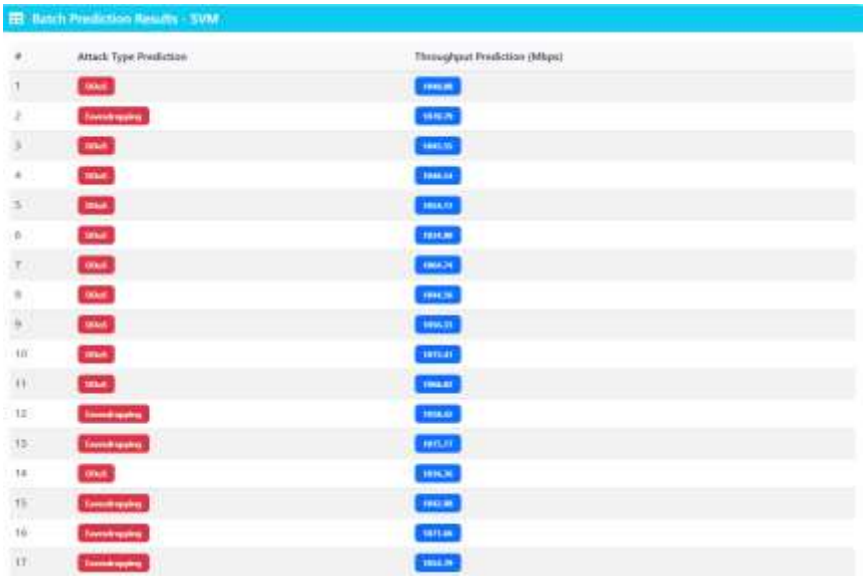


Figure 6: Predictions on test data using proposed TAO model

Figure 6 shows the batch prediction output generated by the system for test data inputs. The results are presented in a tabular format where each record includes the predicted attack type and corresponding throughput value. The predictions are produced after applying consistent preprocessing steps, including encoding and scaling, ensuring accuracy and uniformity across all inputs. This output provides a clear representation of how different network conditions are classified and how throughput is estimated, supporting effective analysis and validation of the system's performance.

5. CONCLUSION AND FUTURE SCOPE

The study presents a web-based ML framework for intelligent network monitoring that performs simultaneous attack classification and throughput prediction using the proposed GNN-SLIM framework together with the existing SVM, KNN, and TAO Tree models. The system integrates data preprocessing, EDA, model training, evaluation, model storage, and real-time prediction within a unified Flask-based application to provide comprehensive analysis of both network security and communication performance. Preprocessing techniques such as Label Encoding, Standardization, and SMOTE are incorporated to improve data quality, feature representation, and learning capability. The dual-task learning framework enables efficient identification of different network attack types while accurately predicting network throughput, providing valuable insights into network behavior. Experimental results demonstrate that the proposed GNN-SLIM framework achieves superior classification and regression performance compared with the existing models by effectively learning complex network traffic characteristics and generating highly accurate predictions.

REFERENCES

[1]. Ismail, W.N. A Novel Metaheuristic-Based Methodology for Attack Detection in Wireless Communication Networks. Mathematics **2025**, 13, 1736. https://doi.org/10.3390/math13111736.

[2]. Kaur, N.; Gupta, L. Securing the 6G–IoT Environment: A Framework for Enhancing Transparency in Artificial Intelligence Decision-Making Through Explainable Artificial Intelligence. Sensors **2025**, 25, 854. https://doi.org/10.3390/s25030854.

[3]. Okere, E.E.; Balyan, V. Sixth Generation Enabling Technologies and Machine Learning Intersection: A Performance Optimization

Doi:10.48047/ijiee.2026.16.2.49

Perspective. Future Internet **2025**, 17, 50. https://doi.org/10.3390/fi17020050.

[4]. Nassreddine, G.; Nassereddine, M.; Al-Khatib, O. Ensemble Learning for Network Intrusion Detection Based on Correlation and Embedded Feature Selection Techniques. Computers **2025**, 14, 82. https://doi.org/10.3390/computers14030082.

[5]. Braeken, An, Diana Deac, Thanh Linh Nguyen, Gürkan Gür, Quoc-Viet Pham, Charithri Yapa, Paola G. Vinueza-Naranjo, Henry Carvajal Mora, Charuka Moremada, and Madhusanka Liyanage. "6G AI security: From fundamentals to offensive and defensive landscape in 6G." IEEE Communications Surveys & Tutorials (2026).

[6]. Shaji, Livin, Yang Luo, Cheng Yin, and Jie Lin. "Machine Learning-Based Physical Layer Security for 5G/6G-Enabled Electric Vehicle Charging Network." Electronics 15, no. 4 (2026): 865.

[7]. Altintaş, Mücahit, Sümeye Nur Karhan, Yasin Emre Tok, Amine Gonca Toprak, and Öykü Berfin Mercan. "When Beneficial Intelligence Turns Hostile: A Survey of Adversarial Threats in AI-Native 6G." IEEE Open Journal of the Communications Society 7 (2026): 3468-3511.

[8]. Alwaisi, Zainab, and Simone Soderi. "Semantic communication-based detection of False Data Injection Attacks in 6G-enabled smart grids." International Journal of Electrical Power & Energy Systems 175 (2026): 111649.

[9]. De Alwis, Chamitha, Ons Aouedi, Jiaming Xu, Shen Wang, Yushan Siriwardhana, Tharaka Hewa, Engin Zeydan, Chamara Sandeepa, and Madhusanka Liyanage. "Federated learning for 6g security: A survey on threats, solutions and research directions." IEEE Communications Surveys & Tutorials (2026).

[10]. Alwaisi, Zainab, Tanesh Kumar, and Simone Soderi. "Robust and energy-aware detection of Mirai botnet for future 6G-enabled IoT networks." Journal of Network and Computer Applications 248 (2026): 104438.

[11]. Tripathi, Abhishek, A. S. Anagha, Aiswarya S. Kumar, Shubham Anjankar, Suresh Balpande, and S. Wilson Prakash. "Enhancing Cybersecurity Resilience in 6G Networks Using Adversarial Machine Learning." In Emerging Perspectives and Applications of Computational Intelligence and Smart Systems, pp. 338-344. CRC Press, 2026.

[12]. Harsora, Riddhi V., Sushil Kumar Singh, R. N. Ravikumar, Deepak Kumar Verma, and Santosh Kumar Srivastava. "A Comprehensive Survey of the 6G Network Technologies: Challenges, Possible Attacks, and Future Research." Generative Artificial Intelligence for Next-Generation Security Paradigms (2026): 305-334.

[13]. Kulkarni, Raghavendra, D. Barani, B. VeeraSekharreddy, and L. Guganathan. "Blockchain Cybersecurity Framework for 5G/6G Industrial IoT: Enhancing Industrial and Healthcare Applications With Neural and Graph Networks." International Journal of Communication Systems 39, no. 9 (2026): e70503.

[14]. Vivekanandan, V., S. Pandiarajan, M. Yogadharani, K. Prema, T. Anandhakrishnan, and M. Kannukkiniyal. "A Cloud-Based Intrusion Detection Data Security BSO-ResNet for Malicious Packet Detection for Malicious Network Congestion in 6G Networks." Journal of Multiscale Modelling (2026): 2640028.

[15]. Anegdouil, Brahim, Anass Sebbar, and Mohammed Boulmalf. "Transformer-Based Web Attack Detection for 6G MEC-Enabled SDN Architectures." In 2026 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1-6. IEEE, 2026.

Doi:10.48047/ijiee.2026.16.2.49