HiLL PUBLISHING

Advances in Computer and Communication, 2025, 6(1), 14-19
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Application of Graph Alignment Double Layer Attention Mechanism in Detecting Malicious Traffic in TLS/SSL Encryption

Hangjiang Guo*, Jinghan Zhang

Beijing University of Posts and Telecommunications, Beijing 100876, China.

How to cite this paper: Hangjiang Guo, Jinghan Zhang. (2025) Application of Graph Alignment Double Layer Attention Mechanism in Detecting Malicious Traffic in TLS/SSL Encryption. *Advances in Computer and Communication*, 6(1), 14-19.
DOI: 10.26855/acc.2025.01.003

Received: December 29, 2024
Accepted: January 27, 2025
Published: February 25, 2025

***Corresponding author:** Hangjiang Guo, Beijing University of Posts and Telecommunications, Beijing 100876, China.

Abstract

This article proposes an innovative malicious traffic detection method for TLS/SSL encryption based on a dual-layer attention mechanism with graph alignment. The method effectively captures both the graph structure and node features of network traffic using structural and feature attention layers. It introduces a session-based traffic graph construction approach and a malicious traffic allocation algorithm to handle complex encrypted traffic patterns. The dual-layer attention mechanism is optimized through a graph alignment process using the Gromov-Wasserstein distance and Sinkhorn algorithm, with local structure preservation constraints. A multi-objective loss function, including graph alignment loss and classification loss, is designed to enhance model training. Experimental results on the ISCX VPN-nonVPN 2016 dataset demonstrate superior performance compared to traditional machine learning and deep learning methods, achieving 98.3% accuracy, 98.5% precision, and 98.1% recall. This approach not only improves the detection capability of encrypted malicious traffic but also provides new insights for addressing increasingly complex network security challenges in encrypted environments.

Keywords

Dual layer attention mechanism; TLS/SSL encrypted traffic; Malicious traffic detection; Graph alignment

1. Introduction

With the widespread use of TLS/SSL encryption, detecting encrypted malicious traffic presents significant challenges. Traditional feature engineering struggles with complex encrypted traffic, while deep learning excels in advanced feature extraction but still faces issues with spatiotemporal structural information and interpretability [1]. This article proposes a malicious traffic detection method using a dual-layer attention mechanism. It transforms network traffic into graph structures, captures structural and feature information, and performs classification. Key contributions include a novel dual-layer attention graph alignment mechanism, a session-based traffic graph construction method, a multi-objective loss function, and experimental validation on public datasets.

2. Methods

2.1 TLS/SSL Encrypted Malicious Traffic Detection Framework Based on Graph Alignment

This study proposes a dual-layer attention graph alignment mechanism, which first transforms network traffic data into a graph structure with nodes as sessions, and establishes edges through temporal, spatial, and protocol correlations. The core dual-layer attention mechanism includes a structural attention layer and a feature attention layer, generating enhanced graph representations. Graph alignment optimization adopts Gromov Wasserstein distance and Sinkhorn algorithm [2], and introduces local structure preservation constraints based on attention weights. In the

classification stage, graph neural networks are used for feature learning, and multi-objective loss functions are used to optimize training, ultimately outputting detection results and confidence levels. This framework effectively enhances its adaptability to encrypted traffic.

2.2 Dual-layer Attention Graph Alignment Mechanism

The dual-layer attention graph alignment mechanism is the core innovation for enhancing malicious traffic detection in TLS/SSL encryption. It features a structural attention layer and a feature attention layer that together capture critical information about graph structure and node features [3]. The structural layer utilizes the message-passing mechanism of graph neural networks (GNNs) to assess node importance, employing Graph Attention Network (GAT) for defining attention coefficients as shown in equation 1:

$$\alpha_{ij} = \mathrm{softmax}_i\left(\mathrm{LeakyReLU}\left(a^T\left[Wh_i \parallel Wh_j\right]\right)\right) \tag{1}$$

where: h_i and h_j are the feature vectors of nodes i and j; W is the weight matrix; a is the attention vector; LeakyReLU is the activation function; $\mathrm{softmax}_i$ represents normalization processing for the neighboring nodes of node i to obtain the attention distribution.

The feature attention layer focuses on the attribute features of nodes, using a self-attention mechanism to assign different weights to different feature dimensions. The calculation process is shown in Equation 2:

$$\beta = \mathrm{softmax}\left(v^T \tanh(Wf)\right) \tag{2}$$

where: f represents the node feature vector; W and v are the parameter matrix and vector of the scientific system, respectively; tanh is the hyperbolic tangent function used to increase non-linearity; softmax is used for normalization processing of feature dimensions to obtain the feature importance distribution.

The outputs of the two attention layers are integrated through weighted summation, as shown in Equation 3:

$$h_i' = \sigma\left(\sum_{j \in N_i} \alpha_{ij} W h_j + \beta_i f_i\right) \tag{3}$$

where: h_i' represents the updated representation of node i; N_i is the neighborhood set of node i; σ is the activation function; α_{ij} and β_i represent the feature transformation result of node j and the original feature of node i, respectively.

This dual-layer attention mechanism can simultaneously consider the structural and feature information of the graph, effectively extracting key features of encrypted traffic while preserving the graph's topological structure [4], providing richer and more accurate graph representations for subsequent malicious traffic detection tasks.

2.3 TLS/SSL Encrypted Traffic Feature Extraction

The construction of a network traffic graph is essential for applying the dual-layer attention mechanism to detect malicious traffic in TLS/SSL encryption. This study uses a session-based graph method to convert network traffic data into a structured representation. Each network session is treated as a node, with attributes from the TLS/SSL handshake, such as cipher suites and certificate information. Edges are formed based on the temporal and spatial relationships between sessions, as illustrated in Figure 1.

The specific design process is as follows:

(1) Temporal correlation edges: Using sliding time window technology, session nodes occurring within a time window Δt are connected, with edge weights calculated as shown in Equation 4:

$$w_t = \exp\left(-\frac{|t_i - t_j|}{\sigma}\right) \tag{4}$$

where: t_i and t_j represent the timestamps of two sessions; σ is the time decay factor, determining the impact of time differences on edge weights.

(2) Spatial correlation edges: Connections are established based on the similarity of source and destination IP addresses, using Jaccard similarity to calculate the similarity degree of IP addresses, with edge weights calculated as shown in Equation 5:

$$w_s = \frac{|IP_i \cap IP_j|}{|IP_i \cup IP_j|} \tag{5}$$

where: $|IP_i \cap IP_j|$ represents the size of the intersection of the two sets; $|IP_i \cup IP_j|$ represents the size of the union of the two sets.

(3) Protocol correlation edges: Connections are established for sessions using the same TLS version or having similar cipher suites, with edge weights calculated using cosine similarity, as shown in Equation 6:

$$w_p = \cos(\theta) = \frac{\vec{A} \cdot \vec{B}}{||\vec{A}|| \cdot ||\vec{B}||} \tag{6}$$

where: $\vec{A} \cdot \vec{B}$ represents the dot product of vectors; $||\vec{A}||$ and $||\vec{B}||$ represent vector constants.

(4) Comprehensive edge weight: The weights of temporal, spatial, and protocol correlation edges are weighted and fused to obtain a comprehensive edge weight, as shown in Equation 7:

$$w = \alpha \cdot w_t + \beta \cdot w_s + \gamma \cdot w_p \tag{7}$$

where: α, β, and γ are adjustable weight parameters used to balance the contribution of different types of edges to the graph structure.

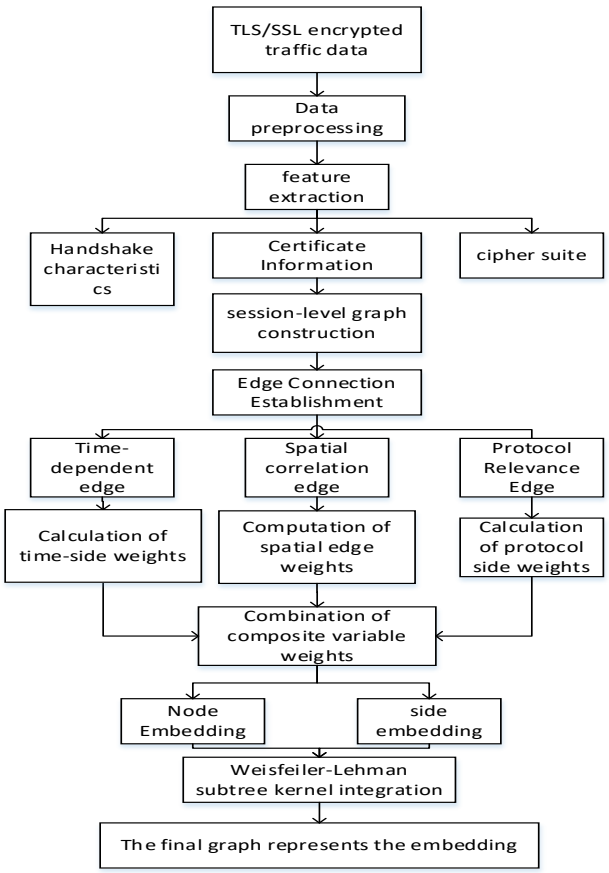

Figure 1. Operating Process.

2.4 Loss Function Design

2.4.1 Graph Alignment Loss

The loss function design in this research aims to optimize the performance of the dual-layer attention mechanism in TLS/SSL encrypted malicious traffic detection [5]. Building on the current design, a graph alignment loss function L_Align is introduced, using the Gromov-Wasserstein (GW) distance to measure the structural similarity between source and target graphs. The GW distance is defined as shown in Equation 8:

$$L_{Align} = \min_T \sum_{i,j,k,l} C_{i,j,k,l} \cdot T_{i,k} \cdot T_{j,l} \tag{8}$$

where: C is the cost matrix; T is the optimal transport matrix.

To improve computational efficiency, the Sinkhorn algorithm is adopted for approximate optimization. Additionally, a local structure preservation constraint based on attention weights is introduced, as shown in Equation 9:

$$L_{local} = \| A_s - T \cdot A_t \cdot T^T \|_F^2 \quad (9)$$

where: A_s and A_t are the adjacency matrices of the source and target graphs, respectively; $\|_F$ represents the Frobenius norm.

2.4.2 Classification Loss

The classification loss L_cls uses the cross-entropy loss function to measure the difference between model predictions and true labels, as shown in Equation 10:

$$L_{cls} = -\sum_i y_i \cdot \log(p_i) \quad (10)$$

where: y_i is the true label of the sample; p_i is the model's predicted probability for sample i.

To address class imbalance issues, a focal loss mechanism is introduced, as shown in Equation 11:

$$L_{focal} = -\sum_i (1 - p_i)^\gamma \cdot y_i \cdot \log(p_i) \quad (11)$$

Where: γ is an adjustable focusing parameter used to enhance learning for difficult samples.

2.4.3 Application of Graph Alignment in Encrypted Malicious Traffic Detection

To further clarify the application of graph alignment loss function design in encrypted malicious traffic detection, this study takes the detection of DGA (Domain Name Generation Algorithm) attacks in encrypted environments as an example to illustrate the specific application process of graph alignment technology. DGA attacks utilize algorithms to dynamically generate a large number of domain names, making it difficult for C&C (Command and Control) servers to be directly blocked, especially in encrypted traffic. The actual application process is shown in Figure 2.

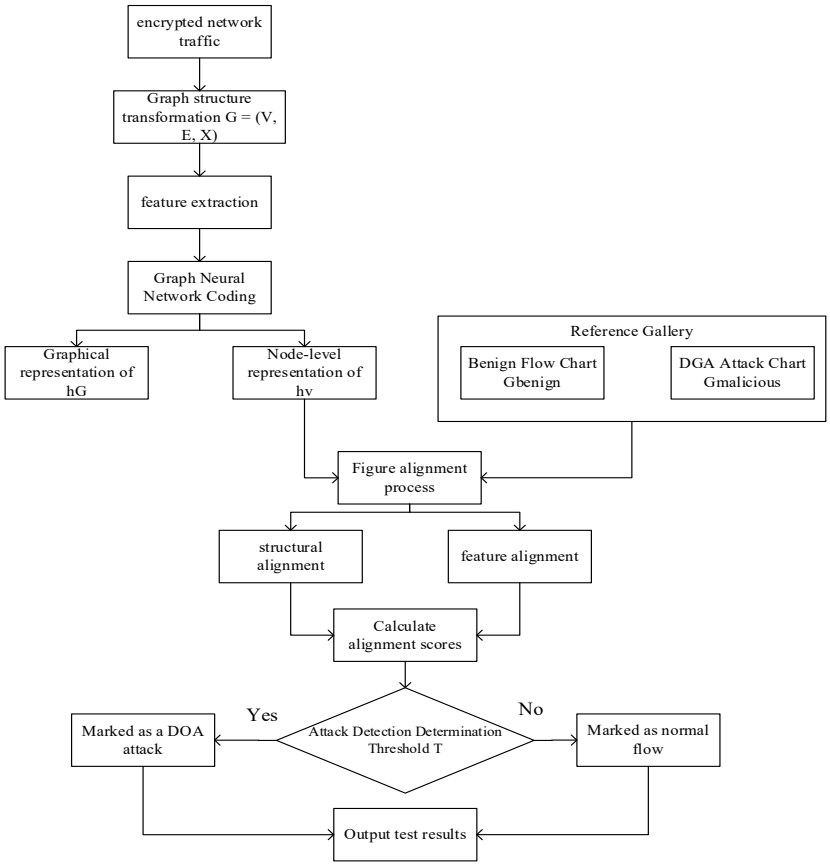

Figure 2. Application Process.

3. Results

3.1 Experimental Setup

The experiment uses the ISCX VPN nonVPN 2016 public dataset, covering various encrypted and nonencrypted traffic. The data is preprocessed, TLS/SSL features are extracted, and a network traffic graph is constructed. The evaluation metrics include accuracy, recall, and F1 score, while the comparison methods cover traditional machine learning (SVM, RF, XGBoost) and deep learning (LSTM, 1D-CNN, GNN). GNN methods include GCN, GAT, and GIN. Simultaneously, a dual-layer attention model without a graph alignment mechanism was implemented as the benchmark. The experiment was conducted using PyTorch on a server equipped with NVIDIA Tesla V100 GPU, using Adam optimizer (learning rate of 0.001, batch size of 64), and conducting 5-fold cross-validation and SMOTE oversampling to solve the problem of class imbalance.

3.2 Result Analysis

The performance evaluation results of the model on the ISCX VPN nonVPN 2016 dataset are shown in Table 1.

Table 1. Model Performance Comparison on ISCX VPN-nonVPN 2016 Dataset

Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	AUC
SVM	91.2 ± 0.3	92.5 ± 0.4	90.8 ± 0.5	91.6 ± 0.4	0.958 ± 0.002
RF	93.5 ± 0.2	94.2 ± 0.3	93.1 ± 0.4	93.6 ± 0.3	0.972 ± 0.001
XGBoost	94.7 ± 0.2	95.3 ± 0.3	94.5 ± 0.3	94.9 ± 0.2	0.978 ± 0.001
LSTM	95.1 ± 0.3	95.8 ± 0.4	94.9 ± 0.5	95.3 ± 0.4	0.982 ± 0.002
1D-CNN	95.8 ± 0.2	96.3 ± 0.3	95.6 ± 0.4	95.9 ± 0.3	0.985 ± 0.001
GCN	96.3 ± 0.2	96.7 ± 0.3	96.1 ± 0.3	96.4 ± 0.2	0.987 ± 0.001
GAT	96.9 ± 0.2	97.2 ± 0.2	96.6 ± 0.3	96.9 ± 0.2	0.989 ± 0.001
Dual-Layer Attention	97.8 ± 0.1	98.1 ± 0.2	97.5 ± 0.2	97.8 ± 0.1	0.995 ± 0.001

Dual-Layer Attention 98.3 ± 0.1 98.5 ± 0.2 98.1 ± 0.2 98.3 ± 0.1 0.997 ± 0.001

The dual-layer attention mechanism effectively detects malicious traffic in TLS/SSL encryption. On the ISCX VPN nonVPN 2016 dataset, it achieved a classification accuracy of 97.8%, outperforming traditional and deep learning methods. The detection accuracy for HTTPS and VPN traffic is 98.7%, surpassing benchmark methods. While the average inference time is 15ms/sample, it remains better than LSTM and 1D-CNN. Overall, these results highlight the superiority of the dual-layer attention mechanism, paving the way for future research.

4. Discussion

The proposed dual-layer attention graph alignment mechanism shows advantages in TLS/SSL encrypted malicious traffic detection, but some issues remain:

(1) Performance varies across traffic types, with VPN detection slightly underperforming HTTPS. Future work could explore more universal graph representations.

(2) The model relies heavily on static features. Incorporating more dynamic behavioral features could improve adaptability to complex attack scenarios.

(3) While effective, the dual-layer attention mechanism increases computational complexity. Future research could focus on more efficient attention designs or model compression techniques.

5. Conclusion

This research provides a new solution for the field of TLS/SSL encrypted malicious traffic detection by innovatively combining the dual-layer attention mechanism with graph alignment theory. The successful application of the dual-layer attention graph alignment mechanism proves the importance of combining structural and feature information,

effectively improving detection accuracy and enhancing the model's adaptability to different types of encrypted traffic. Future research should focus on improving the model's universality, efficiency, and interpretability to address increasingly complex network security environments.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China (NO.62272117) and the National Key Research and Development Program of China (NO.2024YFB31NL00102).

References

[1] Li Y, Ge H. Three dimensional object detection using multimodal data fusion with dual attention mechanism. J Wuhan Univ (Eng Ed). 2024;57(08):1169-1175.

[2] Xie Y, Wang G, Shi N, et al. MSCNN BiLSTM rolling bearing fault diagnosis method integrating attention mechanism. Bearing. 2024;8:86-94.

[3] Wu H, Qian Y, Leng H. Multimodal relation extraction based on bidirectional attention mechanism. Comput Eng. 2024;50(04): 160-167.

[4] Wang W, Chen J, Yang L, et al. Network side alarm sorting method based on multivariate data fusion. J Softw. 2024;35(08):3610-3625.

[5] Shen X, Liu S. Intrusion Detection Method Based on Graph Edge Feature Attention. Comput Eng. 2024 Sep 23;1-11.

[6] Lu R, Wang N, Zhang Y, Lin Y, Wu W, Shi Z. Extraction of Agricultural Fields via DASFNet with Dual Attention Mechanism and Multi-scale Feature Fusion in South Xinjiang, China. Remote Sensing. 2022;14(9):2253.

[7] Hussain F, Abbas SG, Shah GA, Pires IM, Fayyaz UU, Shahzad F, Garcia NM, Zdravevski E. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. Sensors. 2021;21(9):3025.

[8] Xin, L, Ziang, L, Yingli, Z, Wenqiang, Z, Dong, L, Qingguo, Z. TCN enhanced novel malicious traffic detection for IoT devices. Connection Science. 2022;34(1);1322-1341.