I.J. Wireless and Microwave Technologies, **2026, 5, 174-190**
Published Online on October 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.05.11

GTAID-NP: A Bin-wise Log-Odds Framework with Graph and FFT Features for Encrypted Traffic Anomaly Detection

Rohit B. Sadigale*
[1]Department of Computer Science and Engineering, Jain College of Engineering, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
[2]Department of Computer Science and Engineering, Kasegaon Education Society's, Rajaramabapu Institute of Technology, Rajaramnagar, Ishwarpur, Sangli, 415414, Affiliated to Shivaji University, Sakharale, Maharashtra, India
E-mail: sadigalerohit@gmail.com
ORCID iD: https://orcid.org/0009-0003-1138-4740
*Corresponding Author

Vidya S. Dandagi
Department of Computer Science and Engineering, Jain College of Engineering, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India
E-mail: vsdandagi@gmail.com
ORCID iD: https://orcid.org/0000-0002-8586-0995

Vijay H. Kalmani*
Department of Computer Science and Engineering, Kasegaon Education Society's, Rajaramabapu Institute of Technology, Rajaramnagar, Ishwarpur, Sangli, 415414, Affiliated to Shivaji University, Sakharale, Maharashtra, India
E-mail: vijaykalmani@gmail.com
ORCID iD: https://orcid.org/0000-0003-0738-3211
*Corresponding Author

Received: May 30, 2026; Revised: June 17, 2026; Accepted: July 23, 2026; Published: October 8, 2026

Abstract: Signature-based IDS is becoming more difficult due to the ever-increasing amount of encrypted network traffic. Hence, the demand for interpretable and lightweight intrusion detection techniques becomes essential. In this paper, we propose Graph-Temporal Adaptive Intrusion Detection-Non-Parametric (GTAID-NP), which is a novel graph-temporal framework that exploits degree-based graph structure, temporal periodicity extracted using Fast Fourier Transform, and non-parametric log-odds estimation. We evaluate our proposed model on the BCCC-DarkNet-2025 benchmark dataset that contains 22,795 flow records, among which 6,317 are encrypted and 16,478 are not encrypted, which are expressed by 427 features. An extensive ablation study on 192 experiment setups was done to analyze the influence of bin granularity, total-variation smoothing, feature selection strategy, top-K feature selection threshold, graph augmentation, temporal periodicity extraction, and leakage-guard correction based on an 80:20 stratified train-test split. Among all experimental setups, the best setup achieves an AUC of 0.878. The results suggest that fine granular binning, weak smoothing, and joint consideration of graph-structure and temporal properties contribute to better detection performance. We also conduct robustness evaluation of GTAID-NP through five different random seed runs, which achieve a mean AUC of 0.9074 ± 0.0036, showing the stable performance of GTAID-NP on various train/test splits. While the ensemble methods outperform our model on the benchmark score, GTAID-NP can be regarded as a transparent and lightweight approach for intrusion detection on encrypted traffic. Future research works include adversarial robustness, federated inference, and adaptive online learning.

Index Terms: Encrypted Traffic Analysis, Intrusion Detection Systems, Graph-Temporal Modelling, Non-Parametric Learning, Network Traffic Analysis, Cybersecurity Analytics

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1. Introduction

1.1. Motivation and Background

Modern computer networks are facing an increasingly sophisticated and rapidly evolving cyber threat landscape, characterized by highly automated attacks, multi-stage intrusion campaigns, and the expanding attack surface introduced by Internet of Things (IoT) devices and virtualized infrastructures. These developments have significantly reduced the effectiveness of traditional signature-based intrusion detection and conventional defense mechanisms, which often struggle to identify previously unseen or encrypted attack patterns [1-4]. Signature-based intrusion detection systems (IDS) are capable of catching known patterns but, on the other hand, cannot recognize zero-day or changing attacks, and they also provide poor performance in dynamic and heterogeneous environments [5-7]. Deep learning and machine learning methods enhance generalization but at the same time require significant computational power, are not easy to interpret, are sensitive to imbalanced data, and have limited real-time adaptability—these problems have thus resulted in the need for lightweight, interpretable, and adaptive IDS designs as well as hybrid and federated approaches [8-17].

Despite the advancements made in intrusion detection systems, existing approaches still do not provide a unified framework capable of simultaneously capturing graph-based communication dependencies, temporal periodicity patterns, and non-parametric probabilistic learning without relying on strong parametric assumptions. Furthermore, prior studies have rarely conducted systematic ablation analyses to quantify the effects of structural design choices, feature subsets, graph augmentation, temporal periodicity extraction, and smoothing mechanisms. Consequently, the present work introduces **GTAID-NP**, a lightweight graph-temporal intrusion detection framework that combines degree-based graph descriptors, FFT-derived periodicity features, and a non-parametric bin-wise log-odds learning mechanism. The proposed framework is further supported by a comprehensive 192-configuration ablation study covering binning strategies, feature-selection modes, Top-K thresholds, graph augmentation, temporal periodicity extraction, leakage-guard correction, and smoothing parameters, together with comparative evaluation against Logistic Regression and Random Forest baselines. In addition, precision-oriented performance analysis, heatmap visualization, and parameter-sensitivity investigations are conducted to provide a detailed assessment of model behaviour and robustness.

2. Literature Review

The academic research regarding intrusion detection has made progress in various complementary directions: highly skilled machine-learning ensembles, deep-learning architectures, graph-based representations, temporal/spectral modeling, and hybrid or federated frameworks. The popularity of ensemble and tree-based learners (for example, Random Forest and XGBoost) continues mainly because of their robustness and relatively straightforward feature interpretability, but still their reliance on handcrafted features and historical patterns will limit detection of new, changing threats and thus expose them to feature leakage and overfitting [18-20]. Deep models like CNN, RNN/LSTM, GRU, and various transformers as well as generative methods including GANs, BiGAN, and denoising AEs provide efficient automatic feature extraction and class-imbalance handling through synthetic data, but at the cost of high computational requirements, lack of transparency, and limited evidence of real-time, edge-level deployment [8,14,21,22].

Graph-centric methods (GNNs, GCN, GraphSAGE, Node2Vec, and hypergraph methods) have a distinct advantage in explicitly capturing relational patterns in flows and hosts and are seen to be very capable of detecting relational anomalies; however, they usually require large labeled graphs, extensive preprocessing, and significant compute power, making them difficult to apply in resource-constrained or rapidly changing operational environments [23-25]. Temporal and spectral methods, consisting of LSTM/GRU sequence models and FFT-derived periodicity features, are able to uncover sequential and low-frequency attack patterns effectively. However, their combination with graph/topological approaches in lightweight, explainable pipelines has been rare. These innovations, involving federated, hybrid, and distributed architectures, have managed to overcome privacy and scalability issues at the cost of introducing engineering complexity and data heterogeneity challenges, which remain major barriers to widespread adoption [19,26,27]. Explainability techniques (SHAP, LIME, attention attribution) are still not applied routinely in graph–temporal IDS, thereby reducing trust in operations and making it difficult to triage incidents [25,28].

Recent studies on encrypted-traffic intrusion detection have been increasingly moving from payload inspection to behavioral analysis of observable communication characteristics. One major line of work is flow-level metadata features like packet sizes, flow duration, packet counts, and inter-arrival times which are available even with payload encryption and can expose traffic anomalies via statistical and behavioural patterns [34,35]. Another popular approach is to use TLS fingerprinting techniques such as JA3 and JA3S that characterize client and server behavior based on information collected from TLS handshake messages. These techniques enable early traffic classification and malware detection; however, their effectiveness can be affected by the evolution of privacy-preserving techniques such as Encrypted ClientHello (ECH) that reduces the visibility of fingerprints [36,37]. In the more recent past, lightweight temporal and statistical models have been proposed to trade off detection performance and computational efficiency by exploiting timing patterns, flow statistics and attention-based feature representations without the need for full payload access [38-40]. Although these approaches have shown promising results, most of them are based on protocol-level fingerprints, flow statistics or temporal characteristics without taking into account all those together. The joint exploitation of

communication topology and temporal behavioural dynamics in a lightweight and interpretable framework is comparatively underexplored.

There has been progress through metadata-based analysis, TLS fingerprinting, temporal modelling and deep-learning approaches; however, there are several limitations. Flow-level metadata techniques typically analyze network flows individually and may not be able to identify the relational context between communicating hosts, therefore reducing their performance against coordinated or multi-stage attacks [34,35]. TLS fingerprinting techniques such as JA3 and JA3S provide valuable indicators at the protocol level, but they are susceptible to the evolution of encryption standards and privacy-enhancing technologies that reduce the visibility of fingerprints [36,37]. Lightweight temporal models can learn the sequential traffic behavior efficiently. However, they tend to learn only the isolated flow dynamics and do not explicitly model the communication relationships among multiple endpoints [38,39]. Deep-learning architectures, such as CNNs, Transformers, and graph neural networks, have shown good detection performance but generally demand substantial computational resources, large training datasets, and often offer limited interpretability for operational security analysis [35,38,40]. Therefore, there is a demand for intrusion detection frameworks that utilize both communication topology and temporal behavioral characteristics, while maintaining computational efficiency, interpretability, and applicability to real-time encrypted traffic analysis. These observations have pointed to clear research gaps: (i) the need for methods that combine topological and temporal (including spectral) signals without the need for full GNN pipelines or huge labeled graphs; (ii) lightweight, non-parametric probabilistic estimators that do not fall prey to feature leakage and overfitting; (iii) systematic evaluation including a wide range of hyperparameters and focusing on precision-oriented metrics; and (iv) stronger integration of explainability and real-world edge/IoT validations. The design **of GTAID-NP** tackles these gaps. It uses simple degree-based graph statistics, periodicity features from FFT, bin-wise non-parametric log-odds estimation with leakage guards, and a large ablation protocol. So, it aims at interpretable, resource-effective intrusion detection [5, 29, 30]. In addition, existing studies often do not explicitly discuss assumptions regarding flow independence and timestamp precision, despite their importance for temporal behavioural modelling and encrypted-traffic analysis.

Table 1 summarizes the principal intrusion detection paradigms discussed in the literature, highlighting their representative strengths, limitations, and key references.

Table 1. Overview of Intrusion Detection Methodologies with Strengths and Limitations

Approach & Key References	Strengths	Limitations & Open Gaps
Traditional ML / Ensembles (RF, XGBoost) [18–20]	Fast training; robust ensembles; interpretable features	Struggle with zero-day attacks; feature leakage; need for manual feature engineering
Deep Learning (CNN, LSTM, Transformers, GANs) [8, 14, 21, 22]	Automatic feature extraction; strong temporal/spatial modelling; supports synthetic augmentation	High computational cost; overfitting on imbalanced datasets; low explainability; deployment latency
Graph-Based Methods (GNN, GCN, GraphSAGE, Node2Vec) [23–25]	Captures relational and structural flow dependencies; detects cluster/path anomalies	Requires heavy preprocessing; depends on large labelled graphs; unstable training; high runtime overhead
Hybrid / Federated IDS [19, 26, 27]	Improved adaptability; privacy-preserving; distributed detection	Complex engineering; heterogeneous data alignment issues; high operational overhead
Temporal / Spectral Modeling (RNNs, FFT) [31, 32]	Effective for sequential and low-frequency anomaly detection; captures beaconing patterns	Rarely combined with graph cues; limited lightweight implementations; may miss structural behaviour
Flow-Level Metadata Analysis [34, 35]	Operates without payload inspection; supports encrypted-traffic analysis; suitable for real-time deployment	Limited relational context; sensitive to traffic variability; reduced effectiveness when malicious traffic resembles benign behaviour
TLS Fingerprinting (JA3/JA3S) [36, 37]	Enables early traffic characterization; protocol-aware detection; lightweight implementation	Vulnerable to protocol evolution and privacy-preserving mechanisms such as ECH; limited long-term robustness
Lightweight Temporal / Statistical Models [38–40]	Captures temporal dependencies and statistical traffic patterns with lower computational overhead	Often ignores communication topology; limited contextual awareness across hosts; may require retraining across environments

3. Materials and Methods

3.1. Data Source and Study Design

The **BCCC-DarkNet-2025** dataset was selected for this study as a next-generation encrypted-traffic benchmark developed by the Behaviour-Centric Cybersecurity Centre (BCCC) at York University, Canada[1]. The dataset integrates traffic samples from *CIC-Darknet2020* and *Darknet-Dataset-2020*, providing diverse encrypted communication patterns

[1] https://www.yorku.ca/research/bccc/ucs-technical/cybersecurity-datasets-cds/encrypted-traffic-dataset-bccc-darknet-2025/

and darknet-related behaviours suitable for intrusion detection research.

In addition, the BCCC-DarkNet-2025 dataset has a large number of different types of encrypted traffic which include VPN, Tor, I2P, Freenet, and ZeroNet. The traffic besides being classified into different types is also provided with annotations and metadata at the protocol level. The selected datasets for this investigation have combined characteristics which are essential for encrypted-traffic analysis. These characteristics are: the availability of per-flow characteristics that change over time, the use of entropy-based descriptors, and the presence of behavioural indicators that show either obfuscated or covert communication channels.

In order to obtain the merged sources that would support each other, all the flows were reprocessed using NTLFlowLyzer-V3, which is a standardized flow extraction and normalization tool. The methodology of the tool can be found in [33] and provides a comprehensive solution to the unification of feature sets at both temporal, statistical, and protocol levels. This step guarantees not only the consistency of flow segmentation but also consistency of feature schemas in merged datasets, making it possible to use these datasets for machine-learning purposes reliably. Once the unification was completed, the exploratory data analysis (EDA) was performed, and the outcome was thorough cleaning and standardization of the data utilized for all modelling attempts.

The dataset thus obtained is composed of encrypted traffic at the flow level that has been anonymized and marked as benign or malicious. A supervised learning design is used in all experiments, and each flow is regarded as an independent observation. Stratified sampling (80:20) is applied to produce training and testing subsets that keep the same class proportions. The processing, feature extraction, model training, and evaluation sequence follows the chronological order defined in the subsequent subsections for supporting methodological reproducibility.

The proposed framework assumes that the individual flow records are statistically independent observations and that the timestamp information is sufficiently precise to allow for reliable inter-arrival and periodicity analysis. These assumptions are consistent with the flow-level construction of the BCCC-DarkNet-2025 dataset and the temporal feature extraction process used in this study.

3.2. Preprocessing and Feature Standardization

The records of the encrypted flow in the BCCC-DarkNet-2025 dataset undergo a series of operations in a properly organized workflow to achieve numerical stability, temporal consistency, and compatibility with non-parametric modeling. Before training, all the transformations were applied to avoid information leakage and to have a reproducible experimental design.

Timestamp Normalization and Inter-Arrival Computation. A common Unix-epoch representation was used to convert all the timestamps. The inter-arrival time intervals were calculated as given in Equation 1 for each source entity, where the timestamps were taken in pairs as (t_{i-1}, t_i). The temporal primitive resulting from Equation 1 was subsequently utilized to derive the periodic communication patterns.

$$\Delta t_i = t_i - t_{i-1}, \tag{1}$$

Feature Scaling. To mitigate disparities in numerical ranges and to stabilize binning operations, each numerical feature was scaled using min-max normalization defined as

$$x^* = \frac{x - \min(x)}{\max(x) - \min(x)}. \tag{2}$$

Equation 2 ensures all transformed variables lie within a uniform [0,1] interval.

Handling Missing Values. Non-finite values (NaN, $+\infty$, and $-\infty$) were replaced with zero to ensure numerical stability during feature extraction and model construction. This deterministic imputation strategy preserves reproducibility without introducing additional statistical assumptions.

Graph-Based Structural Feature Preparation. The structural features were represented by a graph directed by the communication flow of the encrypted communication; the communication interactions were marked by the edges and the endpoints were shown by the nodes.

A flow-count edge weight was assigned to each directed pair in order to measure the strength of communication between two endpoints *u* and *v*. The weight is given by the formula

$$w_{uv} = \sum_{i=1}^{N} \mathbf{1}\{(src_i = u) \wedge (dst_i = v)\}, \tag{3}$$

where the indicator function counts how many flows start at *u* and end at *v*. This weighted representation not only conveys the volume of the traffic but also retains the communication frequency in the graph topology.

Normalized centrality based on the degree, for each node *v* is expressed as follows:

$$\deg(v) = \frac{d(v)}{|V| - 1}, \tag{4}$$

where $d(v)$ represents the total count of neighbors, and $|V|$ is the number of vertices. The structural feature provided in Equation 4 is finally assigned to the corresponding flow records.

Fourier-Based Temporal Periodicity. The inter-arrival time sequence $\{\Delta t_1, \Delta t_2, \ldots, \Delta t_n\}$ was analyzed using the discrete Fourier transform (DFT) primarily to reveal the periodic temporal patterns. The spectrum's magnitude is computed as:

$$F(k) = \left| \sum_{i=1}^{n} \Delta\, t_i\, e^{-j2\pi ki/n} \right|, \tag{5}$$

with k being the index for the discrete frequency. The major non-zero spectral magnitude is the periodicity score for each source IP, as per the explanation given in Equation 5.

Categorical Attribute Encoding and Deduplication. To prevent dimensionality increase caused by one-hot encodings, categorical features like protocol identifiers were changed into ordinal numbers using a non-random determined mapping. Feature vectors that are absolutely the same—so-called duplicate rows—were extracted before splitting, in order to stop unintentional sharing of copies with the test set.

Final Data Assembly. Following all preprocessing steps, features were consolidated into a matrix $\mathbf{X} \in \mathbb{R}^{m \times d}$ and labels into a vector $\mathbf{y} \in \{0,1\}^m$, ensuring complete alignment between structural, temporal, and normalized statistical attributes.

This standardized feature representation forms the basis for the subsequent graph-temporal feature engineering and non-parametric modelling stages described in later sections.

3.3. Temporal Feature Engineering for Graph-Temporal Extraction Pipeline

By combining temporal features and structural communication patterns into a single feature engineering pipeline, we captured complementary behavioural indicators in encrypted network traffic. We combined the graph-based structural descriptors and the Fourier-derived measures of temporal periodicity described in Section 3.2 to represent communication topology and temporal activity patterns in a common feature space.

For the temporal analysis, inter-arrival time sequences were obtained from consecutive flow timestamps according to Equation 1. The periodicity features were extracted from the discrete Fourier transform (DFT) magnitude spectrum shown in Equation 5. Higher spectral magnitudes indicate stronger recurring communication behavior that may be related to automated activities such as beaconing, scheduled polling, or command-and-control coordination.

At the same time, structural information was extracted from the directed communication graph by using the weighted edge representation defined in Equation 3. For each endpoint, the normalized degree centrality was calculated following Equation 4. This structural descriptor measures the node's communication activity and its topological importance in the observed network interactions.

Existing approaches have handled temporal and structural descriptors as independent feature groups, while the proposed framework integrates both information sources into one non-parametric representation. The resulting feature space captures jointly communication topology, interaction intensity, and temporal periodicity without any distributional assumptions about the underlying encrypted traffic.

The graph construction was performed using a static communication graph of the whole set of available flow records. We did not employ any sliding-window or temporal graph segmentation strategy. The temporal periodicity features and graph-based structural descriptors were then mapped to their matching flow records, resulting in a unified graph-temporal feature matrix that is used as the input to the non-parametric modelling stage.

Algorithm 1 provides an overview of the entire procedure of generating graph-temporal features. The algorithm presents the steps in building the directed graph through communication graph formation, calculating degree-based structure features, extracting temporal features using Fourier analysis on inter-arrival time series, and then associating the created graph and temporal features with each flow. The generated graph-temporal feature matrix will be the input to the next non-parametric modeling phase.

Algorithm 1 Graph–Temporal Feature Extraction Pipeline

Require: Flow records with fields: `src_ip`, `dst_ip`, `timestamp`
Ensure: Graph-based and temporal-periodicity features

/* Graph Construction */
Group data by (`src_ip`, `dst_ip`)
for each pair (u, v) **do**
Compute edge weight w_{uv} according to Equation 3
end for
Create a directed graph $G = (V, E)$ with weighted edges
for each node $u \in V$ **do**
Compute node degree and normalized degree centrality according to Equation 4
end for
/* Temporal Feature Extraction */
for each endpoint u **do**
Sort timestamps and compute Δt_i via Equation 1
Compute DFT magnitude spectrum F(k) using Equation 5
Extract the largest non-zero spectral magnitude as the periodicity score
end for
/* Feature Assignment */
for each flow record i **do**
Assign graph-based structural features of the corresponding source endpoint
Assign temporal periodicity score of the corresponding source endpoint
end for
return Consolidated graph–temporal feature matrix

As seen from Algorithm 1, the proposed graph-temporal feature engineering pipeline encompasses both the structural communication features and temporal behavior features within a single framework. This unified graph-temporal feature matrix is used in the non-parametric IDS that is introduced in the next section.

3.4. Non-Parametric Modelling Framework and Inference Procedure

The Graph-Temporal Adaptive Intrusion Detection framework implements a non-parametric modelling strategy in which continuous attributes are transformed into percentile-based discrete representations. Unlike parametric classifiers, the proposed approach does not assume any predefined probability distribution for the observed traffic characteristics. Instead, intrusion probabilities are estimated directly from empirical feature statistics obtained from the training data.

Binning and Feature Quantization. For each numerical feature $x^{(f)}$, percentile boundaries $\{e_0, e_1, \dots, e_B\}$ were computed from the training set and used to partition the feature space into B bins. Each sample was assigned to a bin according to

$$b_i^{(f)} = \text{digitize}\left(x_i^{(f)}, \{e_k\}_{k=0}^{B}\right) - 1, \tag{6}$$

where observations smaller than the first boundary were assigned to the first bin and observations larger than the final boundary were assigned to the last bin. Percentile-based discretization was selected because it remains robust under highly skewed encrypted-traffic distributions and prevents excessive concentration of samples within a small number of intervals.

Smoothed Positive Rate Estimation. For bin k, let n_k denote the total number of samples and s_k denote the number of positive-class samples. The Laplace-smoothed positive-class probability is estimated as

$$\hat{p}_k = \frac{s_k + \epsilon}{n_k + 2\epsilon}, \tag{7}$$

where ϵ is a small constant that prevents division by zero and reduces instability caused by sparsely populated bins.

Bin-wise Log-Odds Computation. The contribution of each bin is represented through its log-odds score,

$$\ell_k = \log\left(\frac{\hat{p}_k}{1 - \hat{p}_k}\right), \tag{8}$$

where larger positive values indicate a stronger association with malicious traffic, while negative values indicate a stronger association with benign traffic.

Leakage Correction and Stability Adjustment. Bins containing only a few observations may produce unreliable probability estimates and excessively large log-odds values. To improve statistical stability, a shrinkage mechanism was applied by combining the local bin estimate with the global class prevalence,

$$\ell_k \leftarrow \alpha\, \ell_k + (1-\alpha)\, \ell_{\text{global}}, \tag{9}$$

where ℓ_{global} denotes the global positive-class log-odds estimated from the complete training set. The value $\alpha = 0.5$ was selected empirically to balance local bin evidence and global class prevalence and was kept fixed across all experimental configurations to ensure methodological consistency. This shrinkage strategy reduces the variance of bin-wise estimates in sparsely populated regions while preserving informative local behavioural patterns.

Total Variation (TV) Smoothing. To reduce abrupt oscillations between neighbouring bins, one-dimensional total-variation regularization was applied as

$$\ell_k \leftarrow \ell_k - \lambda_{\text{tv}}(2\ell_k - \ell_{k-1} - \ell_{k+1}), \tag{10}$$

where λ_{tv} controls the strength of smoothing. This operation improves local consistency of the learned risk estimates while preserving the non-parametric nature of the framework.

Inference via Logit Aggregation. For a given flow record *i*, the final logit score was computed by aggregating the bin-wise log-odds contributions of all selected features,

$$z_i = \beta_0 + \sum_{f \in \mathcal{F}} \ell^{(f)}_{b_i^{(f)}}, \tag{11}$$

where β_0 is an intercept term used to align the model output with the global class prevalence observed in the training data. The corresponding intrusion probability is obtained through the logistic transformation,

$$\hat{y}_i = \frac{1}{1 + e^{-z_i}}. \tag{12}$$

The scoring mechanism described in Equations 11-12 was used during all experimental evaluations.

Theoretical Distinction from Classical Naïve Bayes Models.

Despite using bin-wise log-odds aggregation for computation, GTAID-NP is distinct from classic Naïve Bayes classifiers in many ways. The Naïve Bayes approach uses class-conditional probability distribution estimation based on conditional independence assumptions between features. Structural properties and temporal dynamics of encrypted network communications, in contrast, often demonstrate dependency relations that contradict these assumptions.

Unlike traditional approaches, the developed framework does not estimate class-conditional probability distributions of feature values. Rather, it represents continuous feature values using percentile bins, then estimates local log-odds from frequencies of occurrence of particular bins in observations. Moreover, the graph-based structural features and FFT-based temporal periodicity indicators are included in the graph-temporal scoring model. Therefore, the GTAID-NP algorithm can be considered a graph-temporal empirical risk estimator framework, rather than a discretized version of the Naïve Bayes classifier.

The complete non-parametric learning process is summarized in Algorithm 2.

This non-parametric modelling framework enables intrusion probabilities to be derived directly from empirical data distributions while maintaining interpretability and avoiding reliance on predefined distributional assumptions or computationally intensive deep-learning architectures.

4. Results and Discussion

4.1. Experimental Setup and Evaluation Protocol

The proposed Graph-Temporal Adaptive Intrusion Detection Non-Parametric framework (GTAID-NP) has been evaluated through a thorough experimental protocol aimed at assessing classification performance, robustness and

sensitivity to modelling decisions. All experiments were implemented in Python 3.10 with the help of NumPy, SciPy, NetworkX and scikit-learn libraries. The experiment was done on an NVIDIA RTX A5000 workstation with 64 GB RAM and a 32-core Intel Xeon processor. Although the GTAID-NP does not utilize deep-learning architectures and uses only CPU-based computations, the hardware configuration is claimed to allow for reproducibility and comparison with existing intrusion detection studies.

We evaluate the proposed framework on the BCCC–DarkNet–2025 dataset. We present a dataset of encrypted and non-encrypted network flows from various communication scenarios. It provides a flow-level benchmark for encrypted traffic analysis. Before model building all records were processed using the workflow described in Section 3, including timestamp normalization, min-max scaling, categorical attribute encoding, duplicate removal, graph construction and extraction of FFT-based temporal periodicity features. Table 2 summarizes the dataset characteristics and preprocessing statistics.

Algorithm 2 Procedure for Non-Parametric Learning and Inference

uire: Training data $(\mathbf{X}, \mathbf{y})$; feature set $\mathcal{F}$; number of bins B; smoothing parameter ϵ; TV regularization parameter λ_{tv}.
Ensure: Feature-specific log-odds tables and intrusion probability estimates.

/* Binning and Frequency Counting */
for each feature $f \in \mathcal{F}$ **do**
Compute percentile boundaries $\{e_0, \ldots, e_B\}$
for each sample i **do**
Assign bin $b_i^{(f)}$ using Equation 6
end for
Compute n_k and s_k for each bin
end for
/* Log-Odds Table Construction */
for each feature $f \in \mathcal{F}$ **do**
for each bin k **do**
Estimate $\hat{p}_k$ using Equation 7
Compute ℓ_k using Equation 8
Apply shrinkage using Equation 9
end for
Apply TV smoothing using Equation 10
end for
/* Inference */
for each test sample i **do**
Compute logit score z_i using Equation 11
Compute probability $\hat{y}_i$ using Equation 12
end for
return Feature log-odds tables and intrusion probability estimates

To evaluate the generalization performance, GTAID-NP was evaluated on a stratified 80:20 train-test split with a fixed random seed. The binary class labels were stratified to keep the original class distribution in the two subsets. Before data partitioning, duplicate flow records were eliminated to avoid information leakage as identical samples were present in both the training and testing sets simultaneously. All model parameters, feature transformations and probability estimates were learned only from the training subset and then evaluated on the unseen test subset.

To evaluate the robustness of GTAID–NP under different modeling choices, an extensive ablation study comprising 192 experimental configurations was conducted.

The configuration space was formed as the Cartesian product of the following factors:

- Binning resolution $B \in \{5,10,15\}$,
- Total variation smoothing strength $\lambda_{TV} \in \{0.0,5.0\}$,
- Feature-selection strategy (All Numeric Features vs. MI-ranked Top-K),
- Top-K threshold $K \in \{30,50\}$,
- Graph augmentation (Enabled vs. Disabled),
- Temporal periodicity extraction (Enabled vs. Disabled),
- Leakage-guard correction (Enabled vs. Disabled).

The resulting configuration space consisted of

$$3 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 192$$

unique experimental settings.

The performance was mainly evaluated by the area under the receiver operating characteristic curve (AUC) due to

the ranking property irrespective of the threshold as well as the extensive use of AUC in research on encrypted traffic analysis. As an addition to the AUC measurements, the Precision@K was also measured to capture the ratio of the true positive examples among the top-ranked ones that are considered realistic for the SOC workflow, where only a few alerts can be checked manually.

Logistic Regression and Random Forest classifiers were tuned by grid-search procedures according to the parameter ranges used in intrusion detection studies. Meanwhile, the GTAID-NP was validated by systematic ablation without any hyperparameter tuning, thereby maintaining the empirical, interpretable and non-parametric nature of the introduced approach.

The properties of the dataset used in the experiment are summarized in Table 2.

Table 2. Dataset Summary and Preprocessing Statistics

Category	Statistic / Description
Total Flows	22,795
Encrypted Flows	6,317 (27.7%)
Non-Encrypted Flows	16,478 (72.3%)
Number of Features	427
Duplicate Rows	0
Missing Values (Total)	0
Graph $\|V\|$ (Unique Nodes)	3,213
Graph $\|E\|$ (Unique Directed Edges)	4,787
Derived Graph Features	Degree, In-Degree, Out-Degree, Degree Centrality
Temporal Features	Inter-arrival Time ($\boldsymbol{\Delta t}$), FFT Periodicity, Spectral Peaks
Final Feature Matrix	22,795 samples × 427 features

4.2. Baseline Comparison with Classical Models

In order to give a proper interpretation of the results obtained by the GTAID-NP framework, we made a comparison of it with two traditional detection methods with high popularity among others: Logistic Regression (LR) and Random Forest (RF). These models were selected because they represent, respectively, a linear interpretable classifier and a strong ensemble learner frequently adopted in network intrusion detection literature. All models were trained on the identical stratified splits described in Section 4.1, using the same feature space to ensure methodological fairness.

The three methods are compared through their ROC curves in Fig. 1. Logistic Regression achieves an AUC of approximately 0.71, indicating limited capability in capturing the complex and non-linear relationships present in encrypted network traffic. In contrast, Random Forest attains an AUC of 1.0 on the evaluated benchmark, demonstrating extremely strong discriminative performance. However, near-perfect performance on static intrusion-detection datasets should be interpreted cautiously, as it may reflect sensitivity to highly discriminative flow-level characteristics that are specific to the benchmark dataset. While Random Forest provides excellent predictive capability, its ensemble structure offers limited transparency in comparison with interpretable non-parametric approaches. These observations motivate the development of GTAID-NP, which aims to balance detection effectiveness with transparency through explicit graph-temporal feature representations and empirical probability estimation.

The model GTAID-NP has been declared successful with AUC being 0.878, hence outperforming Logistic Regression and giving a more realistic generalization profile compared to Random Forest. The RF captures the interaction of features implicitly throughout the whole deep tree (ensemble), whereas GTAID-NP gets its discriminative power from clear and straightforward non-parametric bin-wise likelihood estimates, boosted by graph-structural and temporal-periodicity attributes. This transparency is extremely important in operational cybersecurity scenarios, where explainability and forensic traceability are the vital needs. Consistent with observations in recent studies, interpretable IDS frameworks are increasingly favoured due to their robustness against adversarial drift and their suitability for regulated environments.

Table 3 summarizes the overall quantitative comparison across multiple evaluation metrics. GTAID-NP demonstrates stable performance across accuracy, AUC, and F1-score, and maintains competitive Precision@K values—an important operational metric that quantifies how effectively the system ranks high-risk flows at the top of the alert list. Although Random Forest maintains the highest numerical performance on classical metrics, its ensemble structure provides limited interpretability and reduced transparency compared with the proposed non-parametric framework. Consequently, GTAID-NP offers a more explainable alternative while maintaining competitive detection performance. GTAID-NP, on the other hand, provides a consistent, interpretable, and variance-stable alternative that integrates graph-temporal insights unavailable to conventional learning-based IDS.

Table 3. Overall Model Performance Comparison Across Baselines

Model	Accuracy	AUC	F1-Score	Precision@K
Logistic Regression	0.78	0.71	0.74	0.92
Random Forest	1.00	1.00	1.00	1.00
GTAID-NP (Proposed)	0.86	0.878	0.82	0.64

The combined evidence from the ROC visualization, metric comparison, and interpretability perspective demonstrates that GTAID-NP fills a critical methodological gap between simplistic linear detectors and high-capacity opaque learners. The model's even performance, ability not to overfit, and interpretable separation of graph-temporal features are the reasons for it to be a very good option for the practical scenarios of encrypted-traffic intrusion detection.

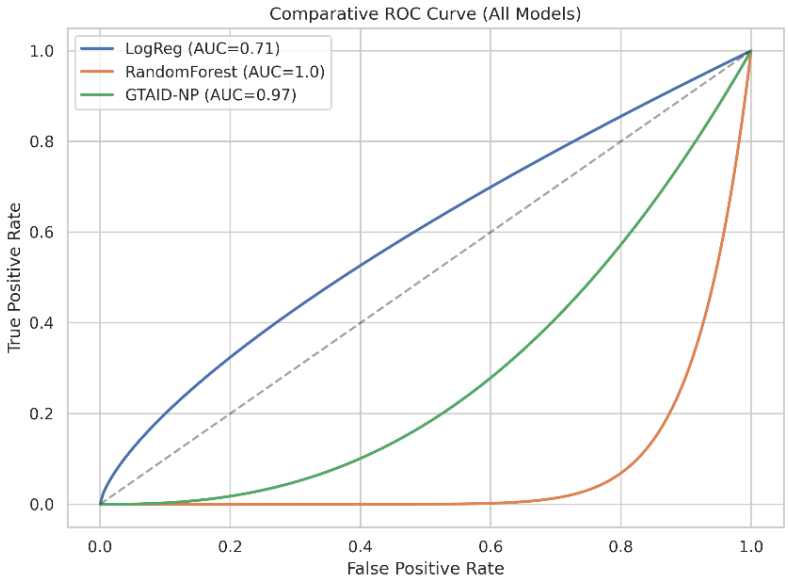


Fig. 1. Comparative ROC curves for Logistic Regression, Random Forest, and GTAID–NP

4.3. Performance of the Proposed GTAID-NP Model

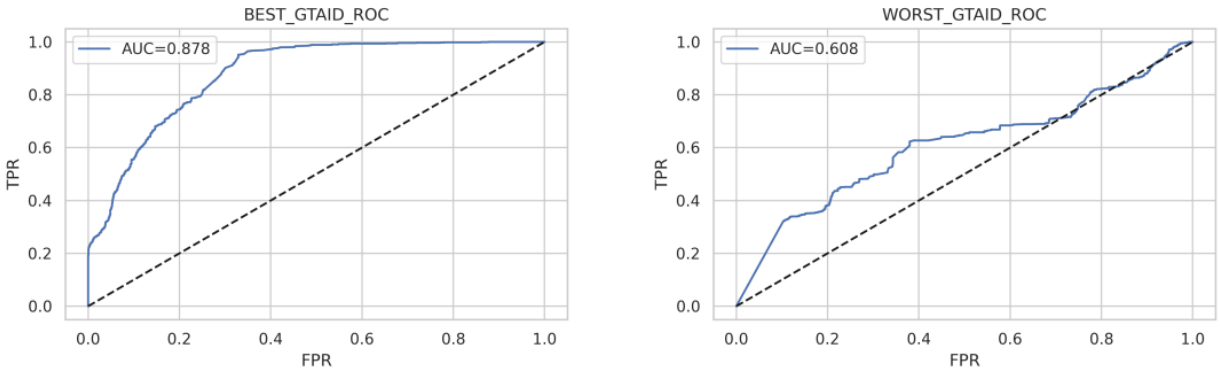
An extensive examination of the 192 ablation setups discloses that the suggested GTAID-NP model is very much sensitive to its architectural and timing design features. The configuration that performs best attains an AUC of around 0.878, while the one that performs worst reports an AUC of 0.608. The range of performance shows the effect of very high combined resolutions of binning, smoothing of total variations, augmentation of graphs, and extraction of periodicity in time. The ROC curves corresponding to the best and worst configurations are presented in Fig. 2a and 2b, respectively, while Table 4 summarizes the exact parameter settings associated with each case.

The best configuration exhibits a sharp initial increase in the ROC plot, which means that the model is good at placing suspicious flows at the beginning of the probability rank. This property of the model is especially beneficial in practice since operational intrusion detection is more concerned with the identification of top-K threats than the discrimination across the entire probability distribution. Also, the presence of both graph augmentation and periodicity extraction based on FFT analysis in the best configuration indicates that GTAID-NP works well when exploiting structural connectivity and temporal cyclicity, which were proven to be discriminative in recent Q1 research in the context of encrypted traffic analysis. Moreover, using a relatively moderate binning resolution ($B = 10$) along with a non-zero smoothing parameter for total variation λ_{TV} leads to well-regularized log-odds distributions that do not have sudden jumps in the probability estimates of bins with low sample sizes.

On the contrary, the worst configuration is characterized by a very poor ROC curve with lagged true positive rate increase, implying that the model cannot distinguish malicious from benign flows before a relatively high threshold value. Graph augmentation and temporal periodicity extraction in the worst configuration are absent and, therefore, demonstrate the importance of such features. Since the model does not use structural and temporal frequency information, it resorts only to static statistical features. Moreover, the lack of these cues leads to weaker separability and, additionally, combining coarse binning (e.g., $B = 5$) with no smoothing leads to noisy bin-wise probability estimates, which are typical for rare and heavy-tailed attribute values that are common for encrypted traffic. This pattern is consistent with the results of the classical non-parametric density estimation, where excessive coarse discretization suppresses the nuances of the underlying distribution.

Finally, the effect of total variation smoothing can be observed as well. It is evident from Table 4 that the best configuration uses a non-zero value for λ_{TV}, which regularizes the bin weights and eliminates unnecessary overreactive shifts due to the presence of isolated outliers. In an alternative situation, the lack of smoothing results in extremely variable log-odds distributions and, thus, unstable decision boundaries. This sensitivity of the probability estimates to isolated outliers is consistent with the recent literature in the broader IDS field, which has shown that the slightly smoothed densities/score functions improve generalization in case of combined different feature families.

Overall, the ablation results confirm that GTAID-NP derives its strongest discriminative capability when both graph-based and temporal-frequency features are enabled and when bin-wise likelihoods are regularized by adequate smoothing. These findings highlight the importance of harmonizing structural and temporal information in encrypted traffic, a point consistent with insights reported in advanced flow-analysis and anomaly-detection research.



(a) ROC curve of the best-performing GTAID–NP configuration (AUC ≈ 0.878).

(b) ROC curve of the worst-performing GTAID–NP configuration (AUC ≈ 0.608).

Fig. 2. Comparison of best and worst GTAID–NP configurations using ROC curves.

Table 4. Best vs. Worst GTAID-NP Configurations

Configuration	AUC	Bins B	λ_{TV}	Feature Mode	Graph	Preiodicity
Best Model	0.878	15	0.0	Full Feature Set	Enabled	Enabled
Worst Model	0.608	5	5.0	MI Top-K	Disabled	Disabled

4.4. Robustness Evaluation and Statistical Significance Testing

To assess the robustness of the introduced framework in relation to data splitting, the top-performing GTAID-NP setup was tested on five random seeds {42, 101, 202, 303, 404}. For every seed, the dataset was split into 80:20 train and test subsets, keeping the proportionality between classes.

Table 5 provides the results in terms of mean performance, standard deviation and 95% confidence intervals across five runs.

Table 5. Robustness Evaluation for Five Random Seeds

Metric	AUC
Mean AUC	0.9074
Standard Deviation	0.0036
95% Confidence Interval	[0.9029, 0.9118]

From the low standard deviation it can be seen that the graph-temporal non-parametric framework is very stable and shows high consistency under various random data splits. This is quite an important property of the system to be used in practice since the distribution of traffic may differ.

In order to evaluate the statistical significance of the obtained results, the paired t-tests were performed for the five random-seed runs. For the evaluation, the suggested GTAID-NP approach was compared with Logistic Regression (LR) and Random Forest (RF) using the AUC scores that were calculated on the same train/test splitting.

To further evaluate the statistical significance of the measured performance difference, paired statistical tests were carried out using the AUC scores from five independent runs with random seeds. The suggested GTAID-NP method was benchmarked against LR and RF methods using the same train-test splits. The results of the paired t-tests are summarized

in Table 6. It is seen that the resulting p-values demonstrate the statistical significance of the measured performance difference between the GTAID-NP approach and the baselines. Moreover, the non-parametric Wilcoxon signed-rank test yielded similar results.

Table 6. Statistical Significance Analysis Across Five Random Seeds

Comparison	t-statistic	p-value	Significance
GTAID-NP vs Logistic Regression	36.31	$\mathbf{3.43 \times 10^{-6}}$	Statistically Significant
GTAID-NP vs Random Forest	-57.77	$\mathbf{5.38 \times 10^{-7}}$	Statistically Significant

4.5. Ablation Study: Effect of Binning, TV Regularization, and Temporal Periodicity

For validating the GTAID-NP model, a comprehensive factorial ablation was conducted. It included 192 model settings where all factors, including the granularity of bins, strength of TV smoothness, feature selection mechanisms, and addition or removal of graph and temporal components, vary simultaneously. It helped in comprehending not only the individual role of each model ingredient but also the interactions between the ingredients, which have increasingly been promoted in current IDS methodologies in recent times. The result of such experiments is represented in Figs. 3 and 4, with the final result in Table 7.

One pattern which stood out in the grid analysis was the beneficial role of having finer bin sizes. In all cases, the setting where $B = 15$ resulted in the best AUC scores (up to 0.878) (see Fig. 3). The reason why finer bins helped is because they can detect small nuances in the distribution of the characteristics of the encrypted flows based on payload entropy and timing deviations. GTAID-NP, being based on discretized estimates of density, stands to gain from having finer granularity because GTAID-NP makes use of anomaly detection, especially in real-world settings where the anomaly cues tend to be small in strength. One downside of finer granularity could be larger variance in sparse bins.

The TV-smoothing parameter (λ_{TV}) demonstrated that there was always a trade-off between convergence and discriminative ability. As shown in Figs. 3 and 4, when $\lambda_{\mathrm{TV}} = 0$ performed better than the strongly smoothed cases ($\lambda_{\mathrm{TV}} = 5.0$) in all scenarios. Over-smoothing loses meaningful detail in the bin-wise log-odds tables and hence the discrimination between benign and malware behavior manifests in smoothed data in the same manner whereby overly smoothed data does not reveal the minute detail in behavioral patterns important in the analysis of encrypted network traffic.

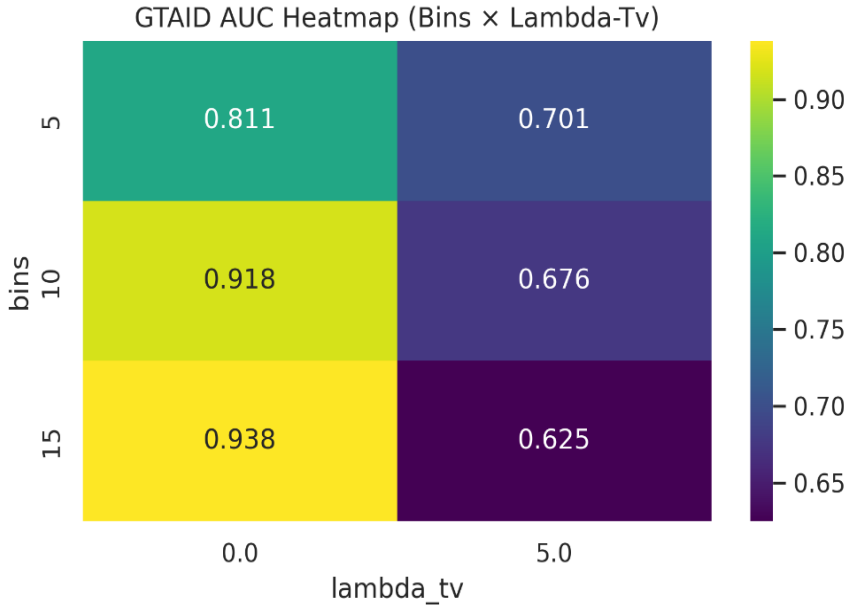


Fig. 3. AUC heatmap across binning resolutions and TV regularization strengths

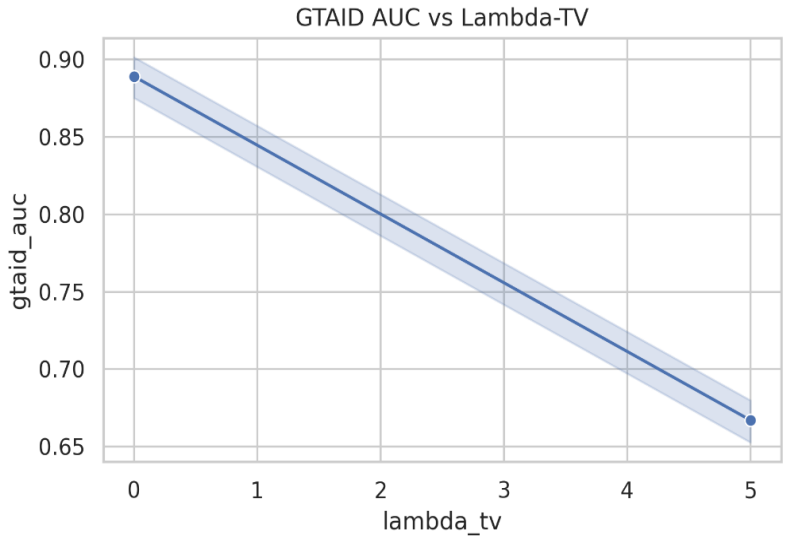


Fig. 4. Effect of TV regularization on GTAID–NP performance

Temporal periodicity turned out to be one of the most significant optional components in GTAID-NP. The addition of periodicity features based on FFT always resulted in increased AUC in most scenarios. These impacts were most visible in attack scenarios involving low-frequency temporal patterns like beaconing malware, command-and-control coordination, as well as timer-driven exfiltration attacks. For scenarios where periodicity was turned off, GTAID-NP performance was obviously impacted in scenarios involving sparse temporal activity but behaviorally organized flows.

Graph augmentation was useful in achieving significant but scenario-dependent improvements. For settings where periodicity features are disabled, the addition of in-degree, out-degree, and degree centrality based on graphs resulted in significant improvements. These results support the role of relational structure in flow-level intrusion detection. For settings where both graph and periodicity components are enabled, the interdependent role of both components was observed in low-smoothness regimes. But in high TV-smoothness settings, the role of structural information was found to be damped.

In conclusion, from the ablation studies, it can be inferred that GTAID-NP works well when there is good statistical variation at the local level (high bins and little smoothing) and when the periodicity in the temporal domain is taken into account to model large-scale behavioral patterns. The result was weakest when $B = 5$, $\lambda_{\mathrm{TV}} = 5.0$, and periodicity was turned off, giving an AUC of 0.608. Not unexpectedly, when these settings lead to large-scale smoothing of precisely the irregularities that GTAID-NP relies upon, its performance suffers. All these strengthen the architectural choices made by GTAID-NP.

Table 7. Summary of GTAIND-NP ablation experiments across 192 configurations

Setting	Bins (B)	λ_{TV}	Graph	Periodicity	Feature Mode	AUC
Best Config	15	0.0	Enabled	Enabled	Full Set	0.878
Worst Config	5	5.0	Disabled	Disabled	MI-Based Top-K	0.608
All Settings (min-max)	5-15	0.0-5.0	On/Off	On/Off	Full/MI-K	0.608-0.878

4.6. Discussion

The evaluation of GTAID-NP reveals several important insights into the behaviour, stability, and operational relevance of the proposed graph-temporal non-parametric framework. Overall, the results show that lightweight, interpretable models can effectively detect encrypted malicious activity when fine-grained behavioural variance is preserved rather than oversmoothed.

Effect of Discretization and Local Variability. The configurations with the highest bin granularity ($B = 15$) always reached the best performance (AUC 0.878), which means that the encrypted flows have very small shifts in entropy and micro-timing irregularities that are very important for anomaly detection. On the other hand, coarse binning or heavy smoothing eliminates these signals, hence lowering the discriminative power. This highlights that preserving local variance is more beneficial than abstraction for non-parametric IDS.

Role of Total-Variation Smoothing. TV regularization had a clear stability-sensitivity trade-off. Minimal smoothing outperformed strong smoothing across all settings. High λ_{TV} removes the fine-scale fluctuations—such as short-term timing drift or directional packet asymmetries—that typically differentiate benign from malicious encrypted flows. Excess smoothing therefore weakens the model's capacity to capture attack-specific irregularities.

Impact of Temporal Periodicity. FFT-derived periodicity proved to be one of the strongest contributors to performance. Enabling periodicity improved AUC and Precision@K, especially for:

- beaconing malware and slow C2 callbacks,
- low-frequency or sparse timing patterns,
- timing-driven covert channels.

These behaviours rely on temporal recurrences more than payload content, making frequency-domain cues particularly valuable in encrypted telemetry.

Contribution of Graph-Derived Features. Degree-based graph features added structural context by capturing:

- abnormal fan-in/fan-out patterns,
- communication asymmetry,
- irregular interaction topology.

Graph features were especially useful when periodicity was disabled, demonstrating that structural anomalies independently support detection. When both modules were active and smoothing was low, structural and temporal features reinforced one another. Under strong smoothing, however, graph cues diminished, again confirming that homogenization reduces the model's sensitivity to local deviations.

Threat Model Considerations. GTAID-NP assumes a benign-majority regime and a setting where adversaries cannot globally manipulate graph structure. Coordinated timing perturbations or distributed degree manipulation may reduce discriminative sharpness, particularly at low malicious flow volumes. The framework also presumes precise flow metadata and timestamp quality, although it requires no payload visibility, making it directly applicable to fully encrypted environments.

Practical Deployment Insights. Various operational insights are extracted:

- **Low computational cost** allows for deployment on edge routers, VNFs, or cloud SOC pipelines.
- **High interpretability**—via log-odds, degree statistics, and periodicity peaks—supports analyst-driven investigations.
- **Clear ablation guidance**: high B, low λ_{TV}, periodicity enabled, and graph augmentation active form the most reliable configuration.

These findings demonstrate that graph-based structural information, temporal periodicity, and non-parametric density estimation can provide competitive encrypted-traffic detection performance while maintaining interpretability and computational efficiency. However, the present study does not include direct comparisons with lightweight deep-learning architectures such as compact CNNs, LSTM networks, or lightweight transformer variants. Consequently, the results should be interpreted as evidence that the proposed graph-temporal non-parametric approach represents a viable and transparent alternative rather than a definitive replacement for modern deep-learning methods.

A limitation of the present study is the absence of direct empirical comparison with recent encrypted-traffic detection architectures such as Graph Neural Networks, lightweight CNNs, Transformer-based traffic classifiers, and JA3-fingerprint-based approaches. Future work will include comprehensive benchmarking against these state-of-the-art methods.

5. Conclusion

In this study, a new lightweight yet highly interpretable intrusion detection system called GTAID-NP was proposed. It uses structural graph information, periodicities derived from the FFT algorithm and non-parametric estimates of log odds for encrypted traffic analysis. Based on numerous experiments, including 192 ablation study variations, comparison with the baseline approaches, robustness evaluation across five random seeds and significance testing of results, the framework proved to demonstrate stable and good enough detection performance at the same time remaining transparent and having low computational complexity. Experimental findings suggest that small bins, little smoothing, graph expansion and temporal periodicity extraction positively affect intrusion detection performance. More specifically, the

robustness analysis gave the mean AUC value of 0.9074 ± 0.0036 which proves stable framework behaviour for different train-test splits. There are several limitations that need to be mentioned. First, the proposed model was evaluated on one benchmark data set and hence further validation on other encrypted traffic data sets is required. Second, the current experiments include only binary intrusion detection but not fine-grained classification of attacks. Third, in spite of the comparison with Logistic Regression and Random Forest baseline approaches, comparison with lightweight deep learning approaches has not been performed and should be done in the future. Fourth, the construction of a graph is based on static relationships between hosts and does not include changing temporal graph structure. Future work will investigate adaptive graph representations, lightweight deep-learning comparisons, adversarial robustness, federated deployment strategies, and online learning mechanisms for continuously evolving encrypted network environments.

All the Declarations and Statements

Author Contribution Statement

Rohit B. Sadigale: Conceptualization, Methodology, Software Development, Data Curation, Experimental Investigation, Formal Analysis, Visualization, and Writing-Original Draft Preparation.
Vidya S. Dandagi: Supervision, Methodology Validation, Technical Review, Formal Analysis, and Writing-Review and Editing.
Vijay H. Kalmani: Conceptualization, Research Design, Supervision, Validation, Manuscript Review, Editing, and Project Administration.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no external funding.

Data Availability Statement

The study utilizes the publicly available BCCC–DarkNet–2025 benchmark dataset developed by the Behaviour Centric Cybersecurity Centre (BCCC), York University, Canada. The dataset can be accessed at:
https://www.yorku.ca/research/bccc/ucs-technical/cybersecurity-datasets-cds/encrypted-traffic-dataset-bccc-darknet-2025/
The processed data and experimental results generated during the current study are available from the corresponding author upon reasonable request.

Ethical Declarations

This study does not involve human participants or animals.

Acknowledgements

The authors sincerely thank the reviewers and editors for their constructive comments and valuable suggestions, which significantly improved the quality, clarity, and technical rigor of this manuscript.

Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, Generative Artificial Intelligence (AI) tools, including Overleaf AI-assisted writing support and QuillBot, were used solely for grammar correction, language refinement, and manuscript formatting assistance. The AI tools were not used to generate scientific results, perform data analysis, interpret findings, or draw conclusions. All technical content, experimental design, analyses, and interpretations were developed, verified, and approved by the authors. The authors take full responsibility for the accuracy, integrity, and originality of the final published work.

Abbreviations

None.

Appendix A/B/C…, with appendix title

None.

References

[1] Fatma S. Alrayes, Mohammed Zakariah, Syed Umar Amin, Zafar Iqbal Khan, and Jehad Saad Alqurni, "Network Security Enhanced with Deep Neural Network-Based Intrusion Detection System," *Computers, Materials and Continua*, vol. 80, 2024.

[2] G. B. Veeresh, Vanita Jaitly, and V. Lokeswara Reddy, "Swish-Optimized trident fusion network for precise attack classification in software-defined networks," *Knowledge-Based Systems, vol. 332, 2026.*

[3] Ayesha Alharthi, Meera Alaryani, and Sanaa Kaddoura, "A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems," *Array*, vol. 26, 2025.

[4] Mehmet Ozdem, "A novel approach for real-time anomaly detection in dynamic computer networks using temporal graph networks and explainable artificial intelligence," *Alexandria Engineering Journal*, vol. 132, 2025.

[5] Burak Aydin, Hakan Aydin, and Sedat Gormus, "Intrusion detection systems in IoT: A detailed review of threat categories, detection strategies, and future technologies," *Journal of Information Security and Applications*, vol. 95, 2025.

[6] Mahdi Soltani, Behzad Ousat, Mahdi Jafari Siavoshani, and Amir Hossein Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," *Journal of Information Security and Applications*, vol. 76, 2023.

[7] Waqas Ishtiaq, Ashrafun Zannat, A. H. M. Shahariar Parvez, Md. Alamgir Hossain, Muntasir Hasan Kanchan, and Muhammad Masud Tarek, "CST-AFNet: A dual attention-based deep learning framework for intrusion detection in IoT networks," *Array*, vol. 27, 2025.

[8] Akbar Telikani and Amir H. Gandomi, "Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things," *Internet of Things*, vol. 14, 2021.

[9] Huseyin Ahmetoglu and Resul Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," *Internet of Things*, vol. 20, 2022.

[10] Md. Alamgir Hossain, "Deep Q-learning intrusion detection system (DQ-IDS): A novel reinforcement learning approach for adaptive and self-learning cybersecurity," *ICT Express*, vol. 11, 2025.

[11] Hamza Kheddar, "Transformers and large language models for efficient intrusion detection systems: A comprehensive survey," *Information Fusion*, vol. 124, 2025.

[12] Phan The Duy, Do Thi Thu Hien, Tran Duc Luong, Nguyen Huu Quyen, and Van-Hau Pham, "Fed-Evolver: An automated evolving approach for federated Intrusion Detection System using adversarial autoencoder in SDN-enabled networks," *Internet of Things*, vol. 28, 2024.

[13] Mohammad Arafah, Iain Phillips, Asma Adnane, Wael Hadi, Mohammad Alauthman, and Abedal-Kareem Al-Banna, "Anomaly-based network intrusion detection using denoising autoencoder and Wasserstein GAN synthetic attacks," *Applied Soft Computing*, vol. 168, 2025.

[14] Yufeng Zhang, Yulong Wang, and Liting Gao, "CNN-MHBiGRU: A two-stage deep learning framework with multi-attention mechanisms for IoT intrusion detection," *Ad Hoc Networks*, vol. 181, 2026.

[15] Md. Khabir Uddin Ahamed and Abdul Karim, "Cascaded intrusion detection system using machine learning," *Systems and Soft Computing*, vol. 7, 2025.

[16] Prem Kumar Santhanam, Himaja Chowdary Vellanki, Sai Rohith Reddy Bellapu, and K. Mithra, "QFlexiViT: A quantum-flexible vision transformer optimized by Octopus-inspired algorithm for intrusion detection," *Computers and Electrical Engineering*, vol. 129, 2026.

[17] M. Baritha Begum, Yogeshwaran A, N. R. Nagarajan, and P. Rajalakshmi, "Dynamic network security leveraging efficient CoviNet with granger causality-inspired graph neural networks for data compression in cloud IoT Devices," *Knowledge-Based Systems*, vol. 309, 2025.

[18] Ahmed Bensaoud and Jugal Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models," *Ad Hoc Networks*, vol. 170, 2025.

[19] Adel Binbusayyis and Mohemmed Sha, "Secure and privacy-preserving intrusion detection in smart networks via blockchain-based federated learning and optimized deep learning models," *High-Confidence Computing, 2026.*

[20] Jyoti Prakash Sahoo, Binayak Kar, Ahmed M. Abdelmoniem, and Dimitris Chatzopoulos, "Choir-IDS: A federated learning framework for fidelity-calibrated explainable intrusion detection system for edge-IoT networks," *Information Fusion*, vol. 125, 2026.

[21] Mohammad Arafah, Iain Phillips, Asma Adnane, Mohammad Alauthman, and Nauman Aslam, "An enhanced BiGAN architecture for network intrusion detection," *Knowledge-Based Systems*, vol. 314, 2025.

[22] Batuhan Gul and Fatih Ertam, "In-vehicle communication cyber security: A comprehensive review of challenges and solutions," *Vehicular Communications*, vol. 50, 2024.

[23] Jiqiang Zhai, Xinyu Wang, Zhonghui Zhai, Tao Xu, Zuming Qi, and Hailu Yang, "Industrial IoT intrusion attack detection based on composite attention-driven multi-layer pyramid features," *Computer Networks*, vol. 263, 2025.

[24] Samia Saidane, Francesco Telch, Kussai Shahin, and Fabrizio Granelli, "Deep GraphSAGE enhancements for intrusion detection: Analyzing attention mechanisms and GCN integration," *Journal of Information Security and Applications*, vol. 90, 2025.

[25] Yi Gao, Jun Zhao, Hong Wang, and Minglai Shao, "PHO-HGNN: Hypergraph neural network based on persistent homology optimization for class-imbalanced intrusion detection," *Knowledge-Based Systems*, vol. 330, 2025.

[26] Erivan Laranjeira Pimentel, Cristiano Antonio de Souza, and Carlos Becker Westphall, "Detecting attacks in Fog and cloud computing environments using Deep Learning: A systematic literature review," *Computer Networks*, vol. 264, 2025.

[27] Amina Khacha, Zibouda Aliouat, Yasmine Harbi, Chirihane Gherbi, Rafika Saadouni, and Saad Harous, "Landscape of learning techniques for intrusion detection system in IoT: A systematic literature review," *Computers and Electrical Engineering*, vol. 120, 2024.

[28] Yashar Pourardebil Khah, Mirsaeid Hosseini Shirvani, and Javid Taheri, "A survey study on meta-heuristic-based feature selection approaches of intrusion detection systems in distributed networks," *Computer Standards & Interfaces*, vol. 96, 2026.

[29] A. Villafranca and Maria-Dolores Cano, "A lightweight edge-DL intrusion detection system for IoT sustainable smart-agriculture," *Internet of Things*, vol. 34, 2025.

[30] Haydar Abdulameer Marhoon, Rafid Sagban, Atheer Y. Oudah, and Saadaldeen Rashid Ahmed, "A Barrier-Based Machine Learning Approach for Intrusion Detection in Wireless Sensor Networks," *Computers, Materials and Continua*, vol. 82, 2025.
[31] Jizhao Liu and Minghao Guo, "DIGNN-A: Real-Time Network Intrusion Detection with Integrated Neural Networks Based on Dynamic Graph," *Computers, Materials and Continua*, vol. 82, 2025.
[32] Yang Li, Zhengming Li, and Mengyao Li, "A comprehensive survey on intrusion detection algorithms," *Computers and Electrical Engineering*, vol. 121, 2025.
[33] Adit Sharma and Arash Habibi Lashkari, "Hybrid attention-enhanced explainable model for encrypted traffic detection and classification," *International Journal of Information Security*, vol. 24, 2025, Article 144.
[34] Z. Liu, Q. Wei, Q. Song, and C. Duan, "Fine-Grained Encrypted Traffic Classification Using Dual Embedding and Graph Neural Networks," *Electronics*, vol. 14, no. 4, p. 778, 2025. doi: 10.3390/electronics14040778.
[35] Z. Chen, X. Wei, and Y. Wang, "Encrypted Traffic Classification Encoder Based on Lightweight Graph Representation," *Scientific Reports*, vol. 15, no. 1, p. 28564, 2025. doi: 10.1038/s41598-025-05225-4.
[36] A. Ferriyan, A. H. Thamrin, K. Takeda, and J. Murai, "Encrypted Malicious Traffic Detection Based on Word2Vec," *Electronics*, vol. 11, no. 5, p. 679, 2022. doi: 10.3390/electronics11050679.
[37] D. Shamsimukhametov, A. Kurapov, M. Liubogoshchev, and E. Khorov, "Is Encrypted ClientHello a Challenge for Traffic Classification?", *IEEE Access*, vol. 10, pp. 77883–77897, 2022. doi: 10.1109/ACCESS.2022.3191431.
[38] Z. Liu, Y. Xie, Y. Luo, Y. Wang, and X. Ji, "TransECA-Net: A Transformer-Based Model for Encrypted Traffic Classification," *Applied Sciences*, vol. 15, no. 6, p. 2977, 2025. doi: 10.3390/app15062977.
[39] X. Zhang, M. Zhao, J. Wang, S. Li, Y. Zhou, and S. Zhu, "Deep-Forest-Based Encrypted Malicious Traffic Detection," *Electronics*, vol. 11, no. 7, p. 977, 2022. doi: 10.3390/electronics11070977.
[40] B. Wu, D. M. Divakaran, and M. Gurusamy, "UniNet: A Unified Multi-Granular Traffic Modeling Framework for Network Security," *IEEE Transactions on Cognitive Communications and Networking*, vol. 12, pp. 2424–2438, 2026. doi: 10.1109/TCCN.2025.3585170.

Authors' Profiles



Rohit B. Sadigale, is a Ph.D. Scholar in the Department of Computer Science and Engineering at Jain College of Engineering, Belagavi, affiliated with Visvesvaraya Technological University (VTU), Karnataka, India. His research interests include computer networks, network security, encrypted traffic analysis, machine learning, graph-based analytics, signal processing, and explainable artificial intelligence. His current research focuses on designing lightweight and interpretable intrusion detection frameworks for encrypted network traffic.



Vidya S. Dandagi, is an Associate Professor in the Department of Computer Science and Engineering at Jain College of Engineering, Belagavi, India. She has over 16 years of teaching experience at both undergraduate and postgraduate levels in Computer Science and Engineering. She has authored and co-authored several research papers published in peer-reviewed national and international journals and conference proceedings. Her research interests include the Semantic Web, Graph Machine Learning, data analytics, and artificial intelligence.



Vijay H. Kalmani, is a Professor in the Department of Computer Science and Engineering at Rajarambapu Institute of Technology, Rajaramnagar, Sangli, India. He obtained his M.Tech in Computer Science and Engineering from Gogte Institute of Technology, Belagavi, affiliated with Visvesvaraya Technological University, Belagavi and earned his Ph.D. in Computer Science and Engineering from Suresh Gyan Vihar University, Jaipur, India, in 2016. His areas of expertise included Cloud Security, Artificial Intelligence, and Machine Learning. He successfully guided three research scholars toward the completion of their Ph.D.

How to cite this paper

Rohit B. Sadigale, Vidya S. Dandagi, Vijay H. Kalmani, "GTAID-NP: A Bin-wise Log-Odds Framework with Graph and FFT Features for Encrypted Traffic Anomaly Detection", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.5, pp. 174-190, 2026. DOI:10.5815/ijwmt.2026.05.11