NTC-CIL: Characterizing and Classifying Encrypted Network Traffic using Class-Incremental Learning

Raju Gudla[*#], Satyanarayana Vollala[#], Ruhul Amin[#], and Mohammad Abdussami[*]

[*]Department of Computer Science & Engineering, SRM University-AP, Amaravati 522 240, Andhra Pradesh, India

[#]CSE Department, International Institute of Information Technology, Naya Raipur, Naya Raipur, 493 661, Chattissgarh, India

e-mail: raju@iiitnr.edu.in, satya@iiitnr.edu.in, ruhul@iiitnr.edu.in, abdussami.m@srmap.edu.in

Abstract: In the field of network security and management, accurately identifying and managing encrypted traffic is essential for mitigating potential attacks and optimizing resource usage. However, conventional methods often underperform in adapting to new traffic classes, require more manual intervention, time-consuming, and resource-intensive. These limitations reduce system performance and increase vulnerability issues. Conventional models also face scalability issues and are prone to catastrophic forgetting, where previously learned traffic patterns are lost as new ones are introduced, leading to reduced classification accuracy over time. To address these challenges, we propose a novel method: Network Traffic Classification using Class-Incremental Learning (NTC-CIL). NTC-CIL combines a random forest classifier with the Learning without Forgetting (LwF) method, an incremental learning method based on knowledge distillation. This approach enables the model to retain previously learned patterns while incorporating new traffic classes, including encrypted and evolving types. As a result, NTC-CIL can continuously adapt to unfamiliar network traffic without retraining from scratch. Experimental evaluations demonstrate that NTC-CIL outperforms existing techniques by achieving an accuracy of 97%. This marks a significant advancement for network security, offering a scalable and adaptive solution capable of detecting new threats in dynamic traffic environments.

Keywords: Encrypted traffic; Class-Incremental learning (CIL); Learning without forgetting (LwF); Random forest classifier; Traffic classification

1 Introduction

In the field of network security and management, accurately classifying network traffic is essential for effective threat detection and mitigation. Traditional techniques based on port numbers and payload inspection have become less reliable due to dynamic port assignments and widespread encryption of information [27]. This has led to a growing need for advanced traffic classification techniques capable of adapting to these evolving challenges. One approach leverages multimedia traffic classification based on both video streaming and network characteristics. Studies have shown a weak correlation between network parameters and perceived video quality. To address this, recent models integrate video streaming parameters with network features to improve classification accuracy [4].

Recent studies have proposed novel models to address encrypted classification. For example, a flow-based geometric learning approach using Graph Neural Networks (GNNs) has demonstrated strong performance in multi-class scenarios by modelling relationships between packets through raw bytes and meta-features [9]. Additionally, adaptive models featuring autonomous updates based on instability checks and familiarity-based filtering have shown promise in maintaining performance across diverse traffic conditions using open datasets [24]. Despite their potential, these approaches often face challenges in scalability and generalizability, especially in dynamic, real-world environments.

To address these challenges, we propose Network Traffic Classification using Class-Incremental Learning (NTC-CIL). This method combines a Random Forest classifier with the Learning without Forgetting (LwF) method, enabling continuous model updates to accommodate new traffic types especially useful for detecting zero-day traffic in an online classification model that accurately identifies both known and previously unseen traffic using statistical features and machine learning.

This paper focuses on traffic classification, identifying the nature of network traffic (e.g., VoIP, streaming, file transfer, and email), which is critical for traffic accounting, Quality of service (QoS) provisioning, and policy enforcement. The NTC-CIL algorithm supports both binary and multiclass classification and adapts over time by integrating new traffic classes without retraining from scratch. It achieves a notable 97% accuracy in classifying traffic, highlighting its potential in real-time encrypted traffic classification.

The main contributions of this research work are as follows:

- We introduce NTC-CIL, a novel approach for encrypted traffic classification at the granularity level.
- The model performs both binary and multiclass classification.
- By incorporating LwF, NTC-CIL ensures the model retains past knowledge while adapting to new traffic, making it suitable for real-time applications.

The rest of this paper is organized as follows: Section 2 introduces the reader to relevant background on encrypted traffic classification approaches. The implementation of the proposed approach is investigated in Section 3. Section 4 describes the experimental setup, the benchmarks, and the tests performed to evaluate our approach. Finally, Section 5 concludes our work and proposes future work.

2 Related Work

This section provides a detailed overview of the main approaches used in classifying encrypted traffic.

The challenge of accurately classifying network traffic, especially unknown has gathered significant attention within the realm of network security. Various techniques have been developed to address this issue, to improve zero-day attack detection performance. The MANTA system, which is built on the multi-lane CapsNet deep learning architecture, addresses the traffic classification problem of identifying and categorizing various network traffic flows. This architecture's advantage is that it enables execution parallelism, enabling each lane to be built independently, greatly enhancing performance in distributed environments [15]. The two innovative discriminators, BitFlow and BitPack, use payload bits as features for machine learning-based traffic classification. BitFlow outperforms ACAS in accuracy and speed, and BitPack offers a user-adjustable balance between privacy and accuracy. Combining BitPack with discriminators like PS and FP further enhances traffic classification accuracy [22]. Festic, a few-shot learning-based strategy to address the low accuracy of present approaches in inadequately labeled traffic. In situations where there is not enough labeled traffic, Festic can reliably classify Internet of Things traffic. During the training phase, Festic gains meta-knowledge from enough labeled IoT flows that are part of the large quantity class[25]. An algorithm for real-time network traffic classification with concept drift using incremental k-means clustering. It analyzes two distance measures (Euclidean and Manhattan) and achieves up to 94% average accuracy. The Manhattan distance-based method classifies network traffic three times faster than Euclidean distance, handling 671,000 flow instances per second [14].

A class-incremental learning (CIL) in deep learning-based traffic classification, focusing on the iCarl method. They identified limitations and proposed an improved version, iCarl+. It uses a softmax activation function and dynamic output layer expansion. However, CIL methods like iCarl+ showed lower performance in traffic classification compared to computer vision, possibly due to small training sets and limited generalization. Further analysis across datasets and exploration of alternative methodologies are needed [3]. An incremental learning framework using OvR and neural network classifiers. It employs a sample selection algorithm to

balance training effort and accuracy when accommodating new applications. Experimental results show the framework achieves incremental learning with high classification accuracy, similar to the closed-world method. The selection algorithm effectively reduces training efforts, meeting dataset scale control and accuracy requirements in lifelong incremental learning [6].

The challenge of efficiently updating deep learning (DL) traffic classifiers due to the rapid release of new mobile applications is addressed in [2]. It explores CIL techniques to add new applications to existing DL-based classifiers without full retraining, aiming to expedite model updates. The study evaluates various CIL approaches using the MIRAGE19 dataset with 40 popular Android applications. While CIL techniques are considered promising, the research indicates their early stage of development in the context of DL-based traffic analysis systems. The significance of machine learning in traffic classification is discussed in [28], especially in identifying encrypted traffic and proprietary protocols by leveraging statistical features. While support vector machines excel in classifying TCP traffic, they have limitations in continuous learning and high resource requirements. A model introduces an incremental Support Vector Machine method to overcome these issues, demonstrating that it reduces training time while maintaining high classification accuracy. Recognizing unknown traffic types using a method that combines multiple features and employs incremental learning. This approach aims to accurately classify traffic that is not previously known to the system. By fusing various features and adopting incremental learning techniques, the study addresses the challenge of identifying unfamiliar traffic patterns in network data [13].

A lightweight framework called "deep-full-range" (DFR) for encrypted traffic classification and intrusion detection using deep learning is introduced in [23]. DFR can train from raw packets without manual intervention. Comparative analysis with state-of-the-art methods using two publically available datasets reveals that DFR excels in performance compared to existing methods by achieving a 13.49% gain in encrypted traffic classification's F1-score and a 12.15% improvement in intrusion detection's F1-score, all while demanding significantly fewer storage resources. The importance of NTC for network security and management purposes, such as QoS provisioning and security. While machine learning (ML) is generally used for NTC, it is unable to overcome limitations due to the insufficient labeled data in real-world applications' traffic. The work investigates the applicability of Active Learning (AL) in NTC, which actively selects instances to be labeled, reducing the need for extensive labeled data. The experimental results show that AL achieves superior performance gain in accuracy with a limited dataset, highlighting its broad strength of application in NTC [17].

A model in [19] focuses on encrypted traffic classification, which is crucial for network management and cybersecurity due to the growth of online applications. It introduces an efficient model, the Cost-Sensitive Convolution Neural Network (CSCNN), that assigns costs to misclassifications based on class distribution to allow for enhancing accuracy. Experiments on the ISCX VPN-nonVPN dataset

show that CSCNN outperforms machine learning and deep learning methods in tasks like traffic classification and application identification. This method offers promising results to the issue of unbalanced data in traffic analysis.

The limitation of catastrophic forgetting in deep CIL, where models tend to forget previously learned knowledge when learning new classes, is discussed in [29]. The classification of recent advances into data-centric, model-centric, and algorithm-centric approaches is performed. They also propose a fair comparison protocol that considers memory budget and memory-agnostic performance measures in evaluating 16 methods for image classification. The study highlights the need for continuous learning in an ever-changing world and the importance of addressing catastrophic forgetting in deep learning models. A survey explores the use of ML techniques for IP traffic classification without relying on traditional TCP or UDP port numbers or packet payload inspection. It reviews 18 significant works from 2004 to early 2007, categorizing them based on their ML strategies and contributions. The paper discusses the motivation for applying ML to IP traffic classification, considers the key requirements for operational IP networks, and highlights open issues and challenges in the field [16].

A challenge of classifying encrypted network traffic is addressed in [18]. It introduces a BERT-based byte-level feature convolutional network (BFCN) with two modules: a packet encoder capturing global features and a CNN capturing local byte-level features. By combining these features, the model achieves state-of-the-art performance on the ISCX-VPN dataset, with F1 score of 99.11% and 99.41% for traffic service and application identification tasks, demonstrating significant improvement in encrypted traffic classification. The research addresses limitations in traditional and deep learning approaches, offering a more effective solution. An efficient multi-task learning approach called the multi-task transformer (MTT) for network traffic classification is discussed in [30]. The MTT simultaneously handles traffic characterization and application identification tasks, reducing complexity and resource demands. Experiments on the ISCX VPN-nonVPN dataset show exceptional results, with F1-score of 98.75% for application identification and 99.35% for traffic characterization, outperforming state-of-the-art models. MTT achieves fast online traffic classification in approximately 0.1 milliseconds per packet. Compared to CNN models, MTT is more stable, offers better classification performance, and requires less storage space.

A model presents a self-supervised method for classifying encrypted network traffic, aiming to minimize the reliance on labeled data, a time-consuming and error-prone task [20]. This model works on a two-stage task, which includes pre-training and fine-tuning, focusing on the need for a significant amount of unlabeled data to achieve high accuracy. Performance evaluation on three datasets reveals the method's ability to outperform state-of-the-art baseline methods by around 3%, particularly when enough data is available during pre-training. And, the approach maintains high accuracy even when trained with unlabeled data from a different dataset, showcasing its robust performance in diverse scenarios. Overall, the

proposed method demonstrates effective classificat-ion of network traffic with minimal labeled data.

A deep learning method for encrypted traffic classification that focuses on protocol-agnostic features like packet size, direction, inter-arrival times, flow statistics, and raw bytes from the TLS handshake [1]. This model employs CNN and stacked long-short-term memory (LSTM) layers. The work finds that incorporating raw traffic beyond the TLS handshake does not improve the model's performance but rather increases complexity and overfitting. Consequently, the suggested feature engineering method relies on universally applicable concepts for encrypted protocols.

An ML technique for classifying networking traffic classification using sub-flows and a gradient-boosted decision tree-based classifier [5]. This method assigns class likelihoods to sub-flows and employs joint likelihood estimations for entire flows, customizable at a certainty threshold. Three classification modes include strict certainty, majority likelihood, and incremental, offering flexibility in categorizing traffic. Evaluation on the Science DMZ subnetwork domain demonstrates 100% accuracy, while the general dataset maintains high accuracy for known traffic but experiences a drop in unknown classification under strict certainty. Flow-Packet Hybrid Traffic Classification (FPHTC), a novel approach for efficient packet-based classification at network routers, is introduced [7]. The FPHTC employs a sophisticated flow-based classifier external to the router, using high-dimensional flow-level features for accurate classification. Simultaneously, a routing policy designer within the router generates a simple policy based on a few packet-level features, leveraging insights from the flow-based classifier. The proposed online routing policy updates ensure FPHTC's robustness to changing traffic patterns. Experimental results demonstrate significant performance improvements in routing policy through knowledge transfer from the flow-based classifier.

A novel feature set derived from Time Series Analysis of Single Flow for versatile binary and multiclass classification [12]. The feature set encompasses statistical deviations in payload lengths and packet times, packet distribution, frequency domain behavior, and specific data point behaviors. Evaluation on 23 network classification tasks with 15 well-known datasets demonstrates the universality of the proposed features, with a reduced set of 10 features suitable for bandwidth-constrained monitoring infrastructures. Over 2500 models are trained and evaluated, showcasing the efficiency of the C++ implementation for rapid integration into flow-monitoring software like ipfixprobe10. A novel approach called the Adaptive Constraint-Driven Classification (AC-DC) framework, addressing the challenge of classifying network traffic at varying rates with limited resources [10]. The AC-DC dynamically adjusts to system resource availability and incoming traffic rates, optimizing performance and classification throughput while adhering to memory constraints. The framework uses a heuristic-based feature exploration algorithm to create a pool of classifiers, selecting the most suitable classifier and batch size based on memory and traffic considerations. Evaluation

results demonstrate superior performance compared to flow-statistics classifiers and significantly higher classification throughput (more than 150x) than conventional packet-capture classifiers. The AC-DC framework is seen as applicable beyond traffic identification, suggesting potential integration into various networked systems for broader problem-solving. Although adaptive streaming classifiers and novel class detection techniques have shown promise in real-time data stream scenarios, they are not directly applicable to our CIL approach. Our method focuses on periodic model updates rather than continuous adaptation, making traditional streaming models less suitable for the current problem statement.

3 Network Traffic Classification using Class-Incremental Learning (NTC-CIL)

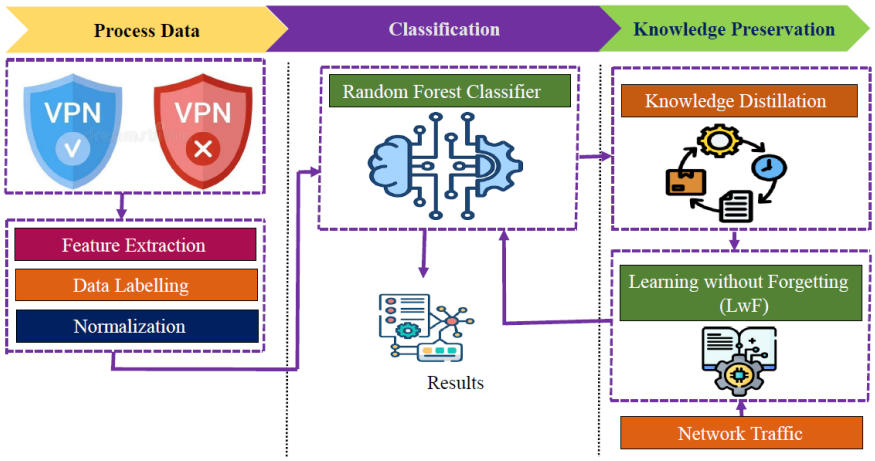

Figure 1
The Proposed NTC-CIL model

The proposed NTC-CIL approach integrates a Random Forest classifier with the LwF method to enable incremental learning. By leveraging traffic statistics and ML techniques, particularly random forest algorithms effectively categorizes unknown packets into one of the categories. The integration of incremental learning empowers the continuous refinement and expansion of the classification model, facilitating adaptation to new traffic classes. The algorithm 1 discusses the procedure of the NTC-CIL and knowledge distillation approaches.

Algorithm 1: Network Traffic Classification using Class-Incremental Learning (NTC-CIL)

Input:

D_old: Labeled dataset of existing traffic classes

D_new: Labeled dataset with new traffic classes

M_old: Pre-trained Random Forest model

λ: Knowledge distillation weight (hyperparameter)

Output:

M_new: Updated model retaining past knowledge

1: Train initial model M_old on D_old
2: For each new class set D_new:
3: Train a temporary Random Forest model M_temp on D_new
4: For each sample x in D_old:
5: y_old ← M_old.predict_proba(x)
6: y_temp ← M_temp.predict_proba(x)
7: Compute distillation_loss = λ * KL_Divergence(y_old || y_temp)
8: Fine-tune M_temp using D_new with distillation_loss
9: Update M_old ← M_temp
10: Return M_new ← M_old

The NTC-CIL approach is designed to update a network traffic classifier to recognize new traffic classes without forgetting previously learned ones. It starts with a Random Forest model trained on existing classes and, when new classes are introduced, trains a temporary model on the new data. To retain old knowledge, it uses knowledge distillation by comparing the predictions of the old and temporary models on old data and minimizing the difference using Kullback-Leibler (KL) Divergence, scaled by a weight factor λ. This helps the new model learn the new classes while preserving the behavior of the original model. The updated model then replaces the old one, resulting in a classifier that can handle both old and new traffic types.

3.1 Class-Incremental Learning (CIL)

CIL is a machine learning approach designed to help models adapt to new classes over time without forgetting previously learned ones. In dynamic environments where class distributions change or new classes appear, traditional models often suffer from "catastrophic forgetting." CIL addresses this by allowing models to learn new information while retaining prior knowledge, maintaining a balance between old and new data. This makes CIL especially models that must continuously evolve to handle emerging traffic types without losing accuracy on known ones.

3.1.1 Learning without Forgetting (LwF)

LwF is an effective CIL technique that helps prevent a model from forgetting previously learned classes when trained on new ones. It does this by incorporating a loss term that encourages the model to retain similar outputs for old classes while learning new data. By using the old model's predictions to guide the training process, LwF preserves prior knowledge and reduces the risk of catastrophic forgetting, making it well-suited for dynamic tasks.

3.2 Dataset Description

Table 1
Dataset Description

Traffic Type	Class (Id)
Non-VPN	Browsing (01), Chat (11), FTP (21), Mail (31), P2P (41), Streaming (51), VOIP (61)
VPN	VPN-Browsing (02), VPN-Chat (12), VPN-FTP (22), VPN-Mail (32), VPN-P2P (42), VPN-Streaming (52), VPN-VOIP (62)

In this research, we evaluate our approach using the VPN-nonVPN dataset [8], which contains network traffic data from both VPN and non-VPN connections. The VPN data capture traffic from various VPN services, offering insights into usage patterns, provider performance, and potential vulnerabilities. The non-VPN portion includes typical internet activities such as web browsing, email, and streaming. This dataset provides a valuable benchmark for analyzing security mechanisms and user behaviour across both environments. A summary of the dataset is provided in Table 1.

3.3 Base Random Forest Classifier

The proposed network traffic classification method uses the CIL technique to overcome the limitations posed by dynamic encrypted network traffic environments. To handle class imbalance, the initial dataset is first resampled using the Synthetic Minority Over-sampling Technique (SMOTE). A Random Forest classifier is then trained on this balanced data, serving as the base model for future knowledge distillation. As new traffic classes are introduced, a new Random Forest model is initialized. Using probability outputs from the base model, the algorithm computes sample weights to guide knowledge transfer. The original resampled data is combined with the new class data, and the new model is trained with a focus on preserving the knowledge of previously learned classes.

The proposed approach uses incremental learning to enable the network traffic classification model to adapt to dynamic changes, including the introduction of new traffic classes. By leveraging knowledge from previous models through knowledge distillation, the algorithm ensures continuous performance improvement. The use

of SMOTE addresses class imbalance, while the integration of new and old knowledge supports effective classification in encrypted and evolving network environments. Its modular design ensures scalability, allowing the model to accommodate new scenarios without the need for full retraining.

3.4 Knowledge Distillation

The Knowledge Distillation algorithm employs the LwF approach to incorporate new classes into an existing traffic classification model. It starts by loading a new dataset containing previously unseen classes and extracting relevant features and labels. A new Random Forest classifier is initialized to ensure unbiased learning. To transfer knowledge from the base model, prediction probabilities are used to compute sample weights, guiding the new model's training process. The algorithm combines the resampled initial dataset balanced using SMOTE with the new dataset and trains the new model on this combined data, with an emphasis on preserving prior knowledge. Finally, the model predicts labels for the new data and evaluates its accuracy, demonstrating the effectiveness of knowledge distillation in adapting to new classes while retaining performance on old ones. This approach enables systematic, adaptive learning and addresses the challenge of evolving network traffic without catastrophic forgetting.

To implement knowledge distillation, we compute sample weights based on the KL divergence between the output probabilities of the base and new models.Thereby, encouraging the new model to mimic the behavior of the original on previously learned classes. The overall loss function is a weighted combination of the standard classification loss and the distillation loss, controlled by a hyperparameter 'λ'. We chose random Forest as the base classifier due to its simplicity, interpretability, and efficiency, making it suitable for real-time or resource-constrained network environments, despite deep learning models being more common in CIL research.

4 Results and Analysis

The continuous updating of the classification model through incremental learning is crucial for maintaining accuracy over time. This adapt-and-learn approach enables seamless integration of new packet classes while preserving existing knowledge, reducing the risk of catastrophic forgetting. Using the NTC-CIL framework, the algorithm achieves a 97% accuracy in classifying new traffic, compared to 90% without Learning without Forgetting (LwF). This significant improvement highlights the algorithms, reliability and effectiveness in real-time network security applications. The high accuracy also reduces false positives and negatives, enhancing overall threat detection. The integration of LwF further strengthens the model's ability to retain prior knowledge while adapting to unknown traffic, demonstrating the robustness of the proposed approach.

In summary, this research introduces an efficient network traffic classification model using the NTC-CIL algorithm, which combines Random Forest with incremental learning to address the limitations of conventional techniques. This approach effectively classifies unseen traffic, demonstrating strong potential for network security applications and laying the groundwork for future advancements in adaptive machine learning for evolving network environments.

The limitations of traditional classification methods highlights the need for innovative approaches. The proposed model, which combines the Random Forest algorithm with incremental learning, continually updates and adapts to new traffic classes. This adaptability results in improved accuracy and makes the model well-suited for dynamic network environments.

Table 2
Performance evaluation of proposed approach without CIL

Class (Id)	Precision	Recall	F1-score
Browsing (01)	0.92	0.90	0.91
VPN-Browsing (02)	0.92	0.82	0.87
Chat (11)	0.90	0.92	0.91
VPN-Chat (12)	0.92	0.83	0.87
FTP (21)	0.98	0.75	0.85
VPN-FTP (22)	0.93	0.84	0.88
Mail (31)	0.92	0.86	0.89
VPN-Mail (32)	0.71	0.94	0.81
P2P (41)	0.95	0.99	0.97
VPN-P2P (42)	0.70	0.96	0.81
Streaming (51)	0.96	0.86	0.91
VPN-Streaming (52)	0.99	0.99	0.99
VOIP (61)	0.99	0.98	0.98
VPN-VOIP (62)	0.98	0.97	0.97

The performance of the proposed approach is presented in Table 2 and Figure 2, showcasing the performance metrics, including precision, recall, and F1-score, for a range of classes in a network traffic classification model. Notably, classes such as P2P (41), Streaming (51), and VOIP (61) exhibit high precision, recall, and F1-score values, indicating the model's effectiveness in accurately identifying and classifying these types of network traffic. On the other hand, VPN-Mail (32) and VPN-P2P (42) demonstrate lower precision and F1-score, suggesting challenges in accurately classifying these categories, particularly in the presence of virtual private network (VPN) networks. The varied performance across different classes underscores the importance of class-specific evaluation metrics in network traffic classification.

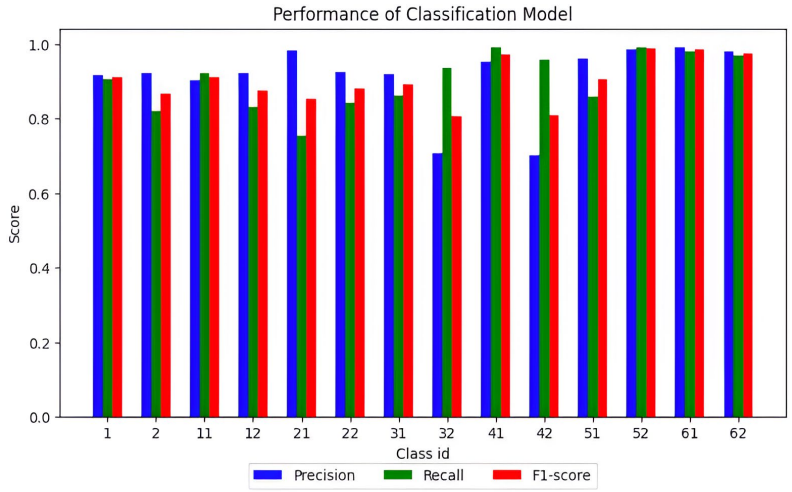

Figure 2

The performance of classification model without CIL

Further analysis and optimization efforts may be directed toward improving the model's performance in classes with lower precision and F1-score, potentially involving additional feature engineering or refining the model architecture to address specific challenges posed by certain traffic types. Overall, these results provide valuable insights into the strengths and weaknesses of the classification model across diverse network traffic categories.

Table 3

Performance evaluation of proposed approach with CIL

Class (Id)	Precision	Recall	F1-score
Browsing (01)	1.00	1.00	1.00
VPN-Browsing (02)	0.99	0.99	0.99
Chat (11)	1.00	0.98	0.99
VPN-Chat (12)	1.00	0.93	0.96
FTP (21)	0.99	0.81	0.89
VPN-FTP (22)	0.96	0.96	0.96
Mail (31)	0.98	0.90	0.94
VPN-Mail (32)	0.94	0.98	0.96
P2P (41)	1.00	1.00	1.00
VPN-P2P (42)	0.74	1.00	0.85
Streaming (51)	0.99	0.89	0.94
VPN-Streaming (52)	1.00	1.00	1.00
VOIP (61)	1.00	0.99	1.00
VPN-VOIP (62)	1.00	1.00	1.00

The performance of the proposed approach with CIL is presented in Table 3, and Figure 3. A comprehensive evaluation of a network traffic classification model revealed high precision, recall, and F1-score values across several classes. Notably, classes like Browsing (01), P2P (41), and VPN-VOIP (62) demonstrate perfect scores, indicating the model's exceptional ability to precisely identify and recall these specific types of network traffic. Conversely, certain classes, such as VPN-Mail (32) and VPN-P2P (42), exhibit comparatively lower precision and F1-score values, suggesting potential challenges in accurately classifying traffic under these categories, particularly when VPN communications are involved. The model maintains robust performance across a diverse set of classes, emphasizing its versatility in handling various types of network activities. These results not only highlight the model's strengths but also provide valuable insights for further refinement, with attention to classes that may benefit from targeted improvements to enhance precision and F1-score metrics. Overall, the evaluation underscores the effectiveness of the classification model while pinpointing areas for potential optimization to ensure robust performance in real-world scenarios. The confusion matrix presented in Figure 4 represents the performance of NTC-CIL on multiclass classification of traffic.

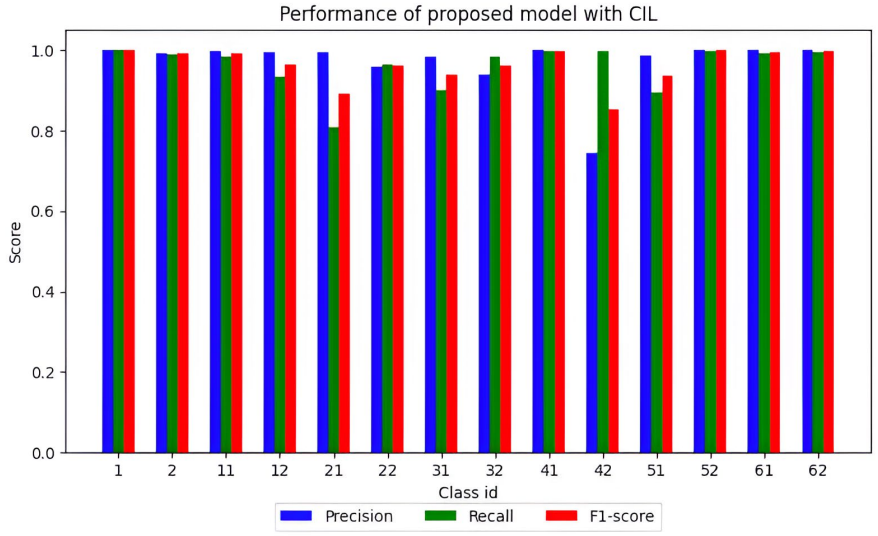

Figure 3
Performance of proposed model with CIL

To evaluate the individual contributions of the key components in our proposed approach, we conducted an ablation study focusing on the LwF method of CIL. We compared the performance of the model with two variants: (i) Without CIL, and (ii) With CIL. The results show that with CIL led to a noticeable high in accuracy due to its impact of class imbalance, while excluding CIL, resulted in increased

forgetting of previously learned classes. These findings highlight the importance of both components in achieving robust and adaptive performance in dynamic network traffic classification.

4.1 Comparison to Existing Approaches

In this section, we compare our results with two state-of-the-art network traffic classification approaches (i.e., Liu Junyi et al.[13], Zhu Wenbin et al.[26]). Figure 5 shows the evaluation results of the three approaches. As shown in Figure 5, we observe that the accuracy of the model in [13] is 86%, and the accuracy of the model in [26] is 94%. NTC-CIL has an overall better classification performance accuracy of 97% outperform [13] and [26], improving about 11% in accuracy. In summary, NTC-CIL outperforms these two state-of-the-art traffic classification approaches under traffic categorization and application identification. The reason is that NTC-CIL uses a method of incremental learning, i.e. LwF. The LwF preserves the classification patterns of the previous information, which are used for further future classification. This cycle of learning and preserving the information continues for the whole classification system. Typically, this classification mechanism is best suited for real-time traffic classification.

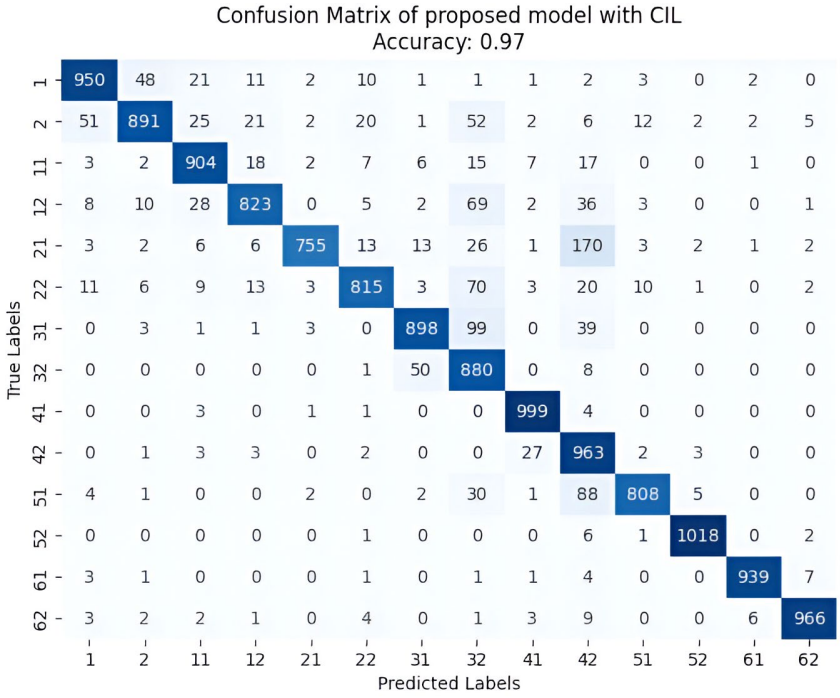

Figure 4
Performance of NTC-CIL on multi-class classification

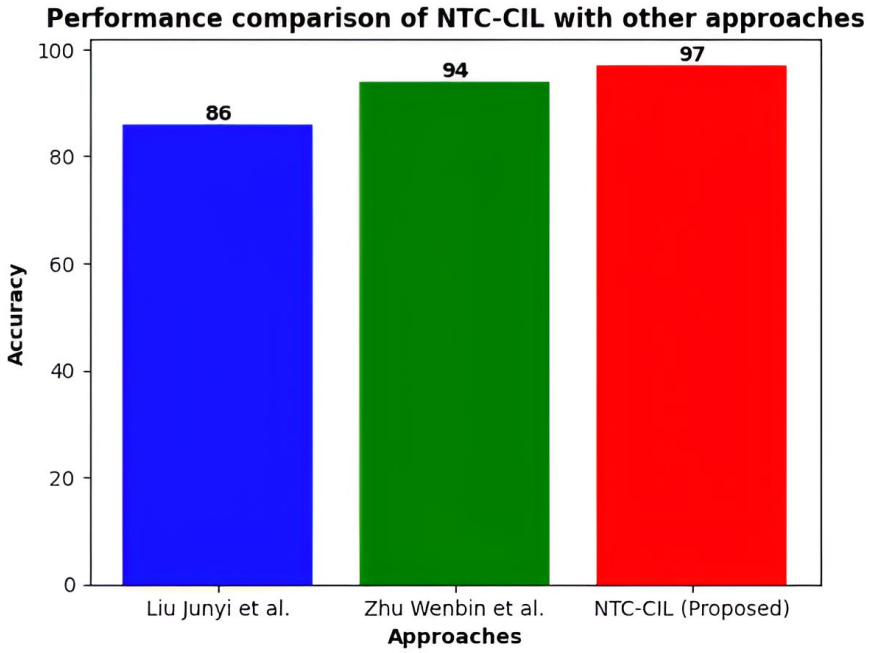

Figure 5
Performance comparison of NTC-CIL with existing methods

Conclusion

The significance of accurate network traffic classification in network security cannot be overstated. Traditional methods are being overshadowed by emerging challenges posed by encrypted communications and dynamic port assignments. This paper proposes a pioneering solution, NTC-CIL. By combining a random forest-based classifier with class incremental learning, the algorithm effectively handles the complexities of unseen traffic classification. The proposed approach outperforms the existing methods with an enhanced accuracy of 97%. This research contributes to advancing traffic classification methods to meet the demand of network security challenges. Future work entails exploring the feasibility of seamlessly integrating the NTC-CIL algorithm into real-time network security systems. This involves a comprehensive investigation into deployment considerations and potential integration challenges to ensure its practical applicability in operational environments. By addressing these critical aspects, the NTC-CIL algorithm has the potential to evolve into a robust and adaptive solution, making significant strides in the advancement of traffic classification.

References

[1] Akbari, I., Salahuddin, M. A., Ven, L., Limam, N., Boutaba, R., Mathieu, B., & Tuffin, S. A look behind the curtain: Traffic classification in an

increasingly encrypted web. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 5(1), 1-26, 2021

[2] Bovenzi, G., Nascita, A., Yang, L., Finamore, A., Aceto, G., Ciuonzo, D., & Rossi, D. Benchmarking class incremental learning in deep learning traffic classification. IEEE Transactions on Network and Service Management, 2023

[3] Bovenzi, G., Yang, L., Finamore, A., Aceto, G., Ciuonzo, D., Pescape, A., & Rossi, D. A first look at class incremental learning in deep learning mobile traffic classification. arXiv preprint arXiv:2107.04464, 2021

[4] Canovas, A., Jimenez, J. M., Romero, O., & Lloret, J. Multimedia data flow traffic classification using intelligent models based on traffic patterns. IEEE Network, 32(6), 100-107, 2018

[5] Chen, J., Breen, J., Phillips, J. M., & Van der Merwe, J. Practical and configurable network traffic classific-ation using probabilistic machine learning. Cluster Computing, 25(4), 2839-2853, 2022

[6] Chen, Y., Zang, T., Zhang, Y., Zhou, Y., Ouyang, L., & Yang, P. Incremental learning for mobile encrypted traffic classification. In ICC 2021-IEEE International Conference on Communications (pp. 1-6) IEEE, 2021

[7] Chowdhury, S., Liang, B., Tizghadam, A., & Albanese, I. Flow-Packet Hybrid Traffic Classificati-on for Class-Aware Network Routing. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6) IEEE, 2021

[8] Draper-Gil, G., Lashkari, A. H., Mamun, M. S. I., & Ghorbani, A. A. Characterization of encrypted and vpn traffic using time-related features. In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP) (pp. 407-414), 2016

[9] Huoh, T. L., Luo, Y., Li, P., & Zhang, T. Flow-based encrypted network traffic classification with graph neural networks. IEEE Transactions on Network and Service Management, 2022

[10] Jiang, X., Liu, S., Naama, S., Bronzino, F., Schmitt, P., & Feamster, N. AC-DC: Adaptive Ensemble Classification for Network Traffic Identification. arXiv preprint arXiv:2302.11718, 2023

[11] Jiang, Z., Lin, R., & Yang, F. An incremental clustering algorithm with pattern drift detection for IoT-enabled smart grid system. Sensors, 21(19) 6466, 2021

[12] Koumar, J., Hynek, K., & ˇCejka, T. Network traffic classification based on single flow time series analysis. In 2023 19th International Conference on Network and Service Management (CNSM) (pp. 1-7) IEEE, 2023

[13] Liu, J., Wang, J., Yan, T., Qi, F., & Chen, G. Unknown Traffic Recognition Based on Multi-Feature Fusion and Incremental Learning. Applied Sciences, 13(13) 7649, 2023

[14] Loo, H. R., Joseph, S. B., & Marsono, M. N. Online incremental learning for high bandwidth network traffic classification. Applied Computational Intelligence and Soft Computing, 2016, 1-1, 2016

[15] Mareri, B., Boateng, G. O., Ou, R., Sun, G., Pang, Y., & Liu, G. MANTA: Multi-lane capsule network assisted traffic classification for 5G network slicing. IEEE Wireless Communications Letters, 11(9) 1905-1909, 2022

[16] Nguyen, T. T., & Armitage, G. A survey of techniques for internet traffic classification using machine learning. IEEE Communications Surveys & Tutorials, 10(4) 56-76, 2008

[17] Shahraki, A., Abbasi, M., Taherkordi, A., & Jurcut, A. D. Active learning for network traffic classificati-on: a technical study. IEEE Transactions on Cognitive Communications and Networking, 8(1), 422-39, 2021

[18] Shi, Z., Luktarhan, N., Song, Y., & Tian, G. BFCN: a novel classification method of encrypted traffic based on BERT and CNN. Electronics, 12(3) 516, 2023

[19] Soleymanpour, S., Sadr, H., & Nazari Soleimandarabi M. CSCNN: cost-sensitive convolutional neural netw-ork for encrypted traffic classification. Neural Processing Letters, 53(5), 3497-523, 2021

[20] Towhid, M. S., & Shahriar, N. Encrypted network traffic classification using self-supervised learning. In 2022 IEEE 8th International Conference on Network Softwarization (NetSoft) (pp. 366-374) IEEE, 2022

[21] Wang, Y., & Nakachi, T. Prediction of network traffic through lightweight machine learning. IEEE Open Journal of the Communications Society, 1, 1919-1933, 2020

[22] Yuan, Z., Xu, J., Xue, Y., & Van der Schaar, M. Bits learning: User-adjustable privacy versus accuracy in Internet traffic classification. IEEE Communications Letters, 20(4), 704-707, 2016

[23] Zeng, Y., Gu, H., Wei, W., & Guo, Y. Deep−F ull−Range: a deep learning based network encrypted traffic classification and intrusion detection framework. IEEE Access, 7, 45182-45190, 2019

[24] Zhang, J., Li, F., & Ye, F. Sustaining the high performance of ai-based network traffic classification models. IEEE/ACM Transactions on Networking, 31(2) 816-827, 2022

[25] Zhao, Z., Lai, Y., Wang, Y., Jia, W., & He, H. A few-shot learning based approach to IoT traffic classification. IEEE Communications Letters, 26(3) 537-541, 2021

[26] Zhu, W., Ma, X., Jin, Y., & Wang, R. ILETC: Incremental learning for encrypted traffic classification using generative replay and exemplar. Computer Networks, 224, 109602, 2023

[27] Fathi-Kazerooni, S., & Rojas-Cessa, R. GAN tunnel: Network traffic steganography by using GANs to counter internet traffic classifiers. IEEE Access, 8, 125345-125359, 2020

[28] Sun, G., Li, S., Chen, T., Su, Y., & Lang, F. Traffic classification based on incremental learning method. In Advanced Hybrid Information Processing: First International Conference, ADHIP 2017, Harbin, China, July 17-18, 2017, Proceedings 1 (pp. 341-348) Springer International Publishing, 2018

[29] Zhou, D. W., Wang, Q. W., Qi, Z. H., Ye, H. J., Zhan, D. C., & Liu, Z. Deep class-incremental learning: A survey. arXiv preprint arXiv:2302.03648, 2023

[30] Zheng, W., Zhong, J., Zhang, Q., Zhao, G. MTT: an efficient model for encrypted network traffic classification using multi-task transformer. Applied Intelligence, 52(9), 10741-10756, 2022