

Conference Paper Title*

*Note: Sub-titles are not captured in Xplore and should not be used

Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Abstract—
Index Terms—

I. INTRODUCTION

The rapid evolution of internet protocols, such as QUIC, HTTP/3, TLS 1.3, and DNS-over-HTTPS (DoH), has introduced significant challenges in encrypted network traffic classification. Traditional Deep Packet Inspection (DPI) methods, which rely on Service Name Indicators (SNI) and DNS queries, are increasingly ineffective in this new landscape. Consequently, the need for innovative classification techniques capable of handling encrypted traffic dynamically and accurately has become more pressing.

Machine Learning (ML) and Deep Learning (DL) models have shown promise in addressing these challenges, serving as benchmarks for encrypted traffic classification. Recent approaches have leveraged diverse data representations, such as transforming network flows into text for Natural Language Processing (NLP) or converting them into images for Convolutional Neural Networks (CNNs). While these methods demonstrate high classification accuracy, they often falter when confronted with previously unseen traffic classes. Existing solutions typically require model retraining to incorporate new classes, a process that is both computationally expensive and time-consuming.

Few-shot learning techniques have emerged as a promising approach to overcome the limitations of traditional classification methods. These techniques aim to classify data using only a small number of labeled examples from new classes, making them well-suited for dynamic and evolving environments like encrypted network traffic. Prototypical Networks, Matching Networks, and Meta-Learning-based models are among the most prominent few-shot learning frameworks. They enable rapid adaptation to new classes by leveraging prior knowledge and focusing on learning effective feature representations.

In addition to few-shot learning, other adaptive classification methods, such as K-Nearest Neighbors (KNN) and its variations, have been employed. Approximate Nearest Neighbors (ANN) methods, for example, reduce computational complexity while maintaining high classification accuracy by

approximating the nearest neighbor search. Classification By Retrieval (CBR), a recent advancement, builds on ANN techniques by combining statistical feature extraction and dynamic retrieval mechanisms to classify new and existing classes in real time without retraining. These methods address the growing demand for scalable, efficient, and adaptive solutions in the realm of encrypted traffic analysis.

While existing approaches have achieved significant progress, the dynamic and encrypted nature of modern network traffic necessitates continued innovation. Robust solutions must not only classify existing traffic accurately but also adapt seamlessly to new traffic patterns and classes without imposing significant computational burdens. This underscores the importance of exploring and refining advanced classification frameworks to meet these challenges effectively.

II. CONTRIBUTIONS

Despite these advancements, there is still room to enhance the adaptability and scalability of these models. In this research, we propose improvements to the CBR algorithm by exploring alternative methodologies for dynamic classification of new classes. Our aim is to develop a solution that achieves high accuracy and efficiency while reducing the computational overhead associated with retraining.

This paper outlines the challenges of encrypted network traffic classification, evaluates existing methodologies, and presents a novel approach to address the dynamic nature of modern internet traffic. By refining adaptive classification techniques, this research contributes to the development of robust and future-proof solutions for encrypted traffic analysis.

III. RELATED WORK

REFERENCES

- [1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955. .