IETF 125 Hackathon

TrafficLLM: Enhancing Large Language Models for Network Traffic Analysis

March 14-20, 2026, Shenzhen

Members: Tianyu Cui, Qi Li, Ke Xu
Zhongguancun Laboratory

IETF

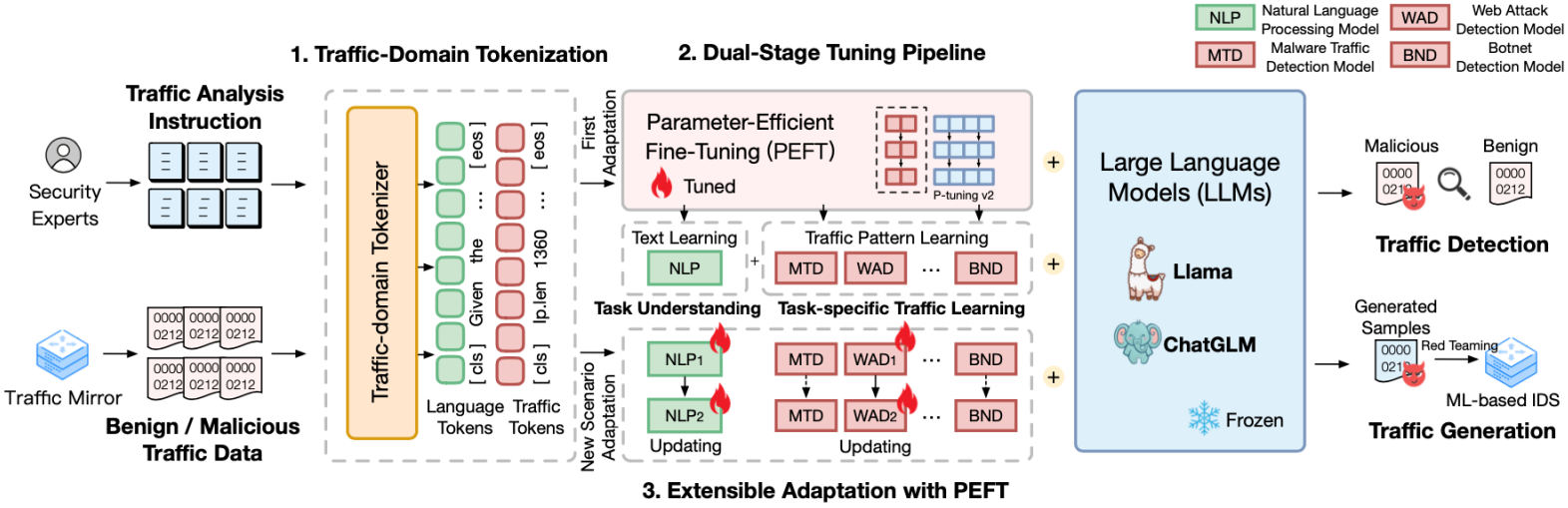
Background

- LLM application to the traffic analysis domain is limited due to the challenge of generalizing to heterogeneous traffic data, different tasks with multimodal learning, and new environments with model update.

Task	Instruction	Response		
Traffic Classification	❶ Please conduct the ENCRYPTED APP CLASSIFICATION TASK to determine which APP category the encrypted traffic belongs to. The categories include 'Adobe, Alipay, ..., and Booking'. <packet>: 04d9... [Encrypted App Classification]	**Gemini:** Based on the provided traffic data, the predicted app category is: Alipay. Explanation: The packet size and structure may resemble previously observed patterns associated with Alipay's protocols ... [Random Guess]	**Claude:** The most likely app category for the provided encrypted traffic is Apple. The packet data contains patterns and characteristics that strongly suggest the traffic is related to Apple services ... [Random Guess]	**ChatGPT:** To determine which class encrypted traffic belongs to based on packet data, a detailed analysis of patterns and features within the encrypted traffic itself is required ... [Only Recommendations]
	❷ The following is a segment of network traffic data, you need to analyze whether it is generated by the communication behavior of malware. If so, please categorize it as Cridex, Geodo, ..., and Zeus. <packet>: 04... [Encrypted Malware Detection]	**Gemini:** The provided packet snippet appears to be a DNS query, but without additional context and analysis, it's difficult to definitively determine if it's generated by malware. However, we can examine ... [Only Description]	**Claude:** Without additional context or analysis, it's difficult to definitively determine if this specific packet is generated by malware communication behavior. However, I can provide an overview ... [Only Description]	**ChatGPT:** Considering the DNS query characteristics, and without additional payload decryption or further traffic analysis, this packet could be related to families like Zeus or Shifu ... [Random Guess]
Packet Simulation	❶ Based on the protocol of fields, traffic features, and payloads of different types of traffic in your knowledge. Please generate a packet of YouTube with the pcap format. [Youtube Traffic Generation]	**Gemini:** Due to the limitations of my knowledge cutoff and the dynamic nature of YouTube traffic, I cannot directly generate a specific packet in hexadecimal format ... [Only Recommendations]	**Claude:** Unfortunately, I cannot generate packet capture (pcap) files or raw network traffic data. As an AI assistant without direct access to network devices or the ... [Only Recommendations]	**ChatGPT:** IP Header: Source IP: 192.168.1.2, Destination IP: 216.58.214.14, Protocol: TCP, TCP Header: Source Port: 49152, Destination Port: 443, Flags: ... [Only Partial Fields]
	❷ I need a packet of Weibo traffic. Based on Weibo's traffic feature, please provide me with a packet of Weibo's traffic data with the pcap format. [Weibo Traffic Generation]	**Gemini:** Unfortunately, due to limitations in my capabilities and knowledge cutoff, I cannot directly generate a pcap file containing Weibo traffic. However, ... [Only Recommendations]	**Claude:** I'm afraid I cannot provide you with an actual packet capture (pcap) file containing Weibo traffic data. As an AI assistant without direct access ... [Only Recommendations]	**ChatGPT:** To obtain a real packet of Weibo's traffic in PCAP format, you would typically use a network traffic capturing tool like Wireshark ... [Only Recommendations]

TrafficLLM

- TrafficLLM is a traffic-domain foundation model to learn generic traffic representation from heterogeneous raw traffic data.
- The framework uses traffic-domain tokenization, dual-stage tuning pipeline, and extensible adaptation to help LLM work on dynamic traffic analysis tasks.



Traffic-Domain Tokenization

- Pre-prompt and heterogeneous feature extraction to build training data.
- Training traffic-domain tokenizer based on BPE.
- **Advantages:** Compared to native LLM, the efficiency and precision has increased by 106% and 17.4%

Traffic Detection Tuning Data Example

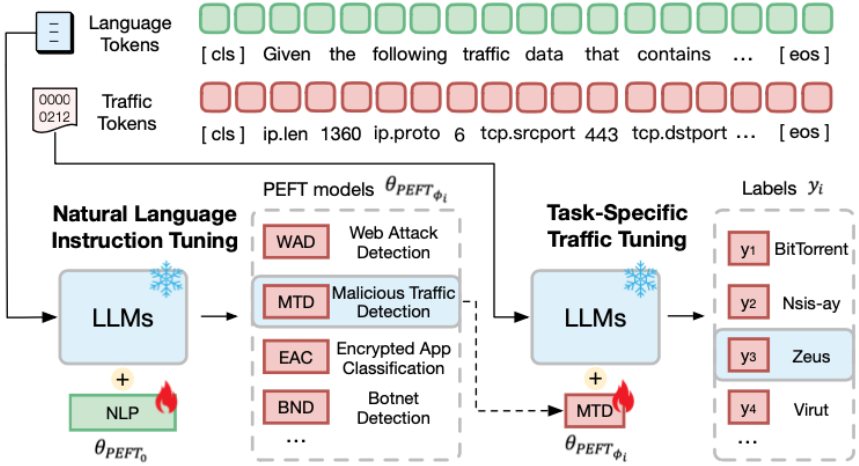
Instruction: Given the following traffic data that contains protocol fields, traffic features, and payloads. Please conduct the Malicious Traffic Detection task to determine which application category the encrypted benign or malicious traffic belongs to.
<packet>: ip.len: 1360, ip.proto: 6, tcp.srcport: 443, tcp.dstport: 56603, tcp.len: 1308, tcp.window_size: ...
Output: Zeus .

Default tokenization: _ip . proto : _ 6 , _ip . che cks um : _ 0 x 0 0 0 0 1 7 a 7 , _ip . che cks um . status : _ 2 , _ip . src : _ 1 0 . 0 . 2 . 1 5 , _ip . d st : _ 1 9 8 . 5 2 . 2 0 0 . 3 9 , _t cp . src port : _ 4 3 7 3 1 , _t cp . d st port : _ 4 4 3 , _t ... [Token length : 1405]

TrafficLLM tokenization: _ip . proto : _6, _ip . checksum : _0 x 000017 a 7, _ip . checksum . status : _2, _ip . src : _10.0. 2.15, _ip . dst : _198.52. 200.39, _tcp . srcport : _43731, dstport : _443, ... [Token length : 690]

Dual-Stage Tuning Pipeline

- Fine-tuning with natural language instructions (FNLI): Understanding instructions and predict downstream task names
- Fine-tuning with downstream-task traffic (FDTT): Learning downstream task traffic patterns and generating prediction results.



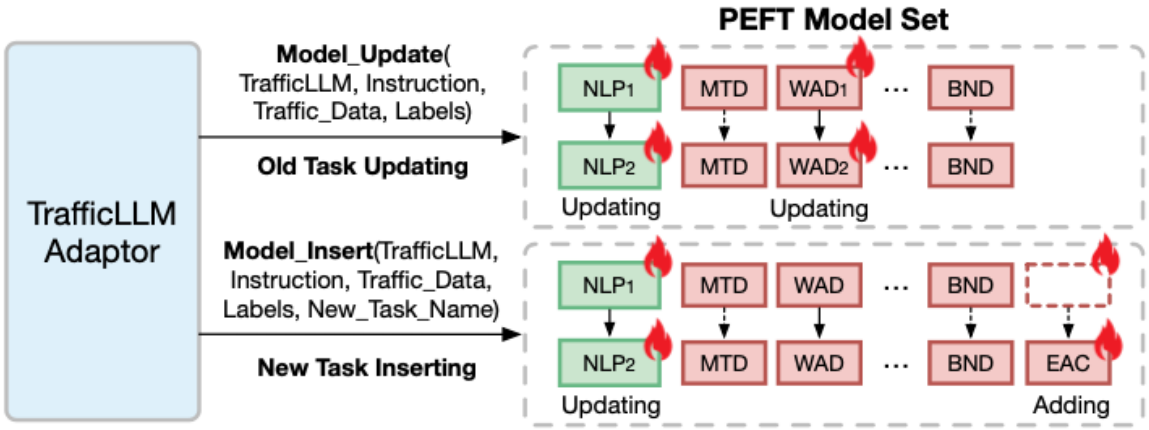
$$\phi_i = \text{TrafficLLM}_{stage_1}(S_i|\theta_1)$$

$$y_i = \text{TrafficLLM}_{stage2}(X_i|(\theta_2;\phi_i \in \phi_{TD}))$$

Advantage: 84.8% Acc improvement compared to directly fine-tuning.

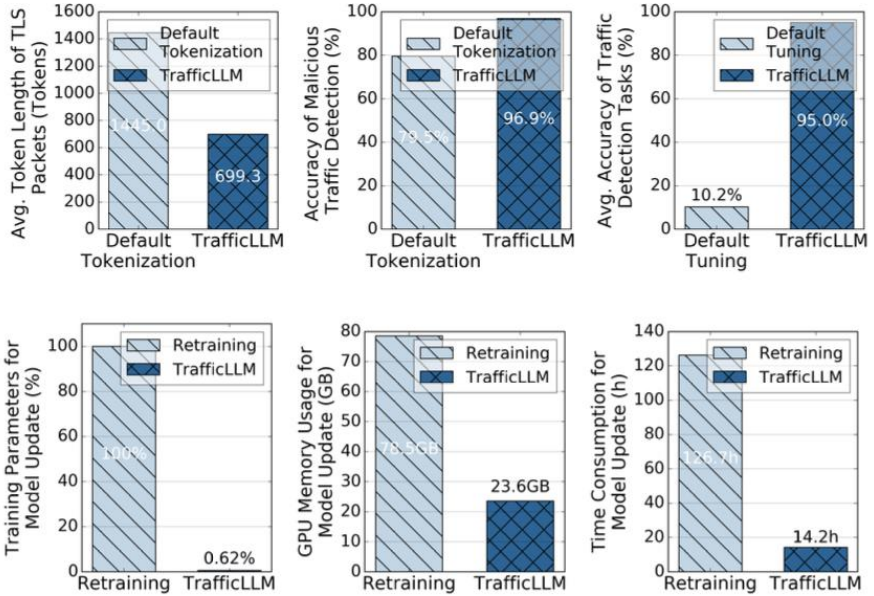
Extensible Adaptation with PEFT

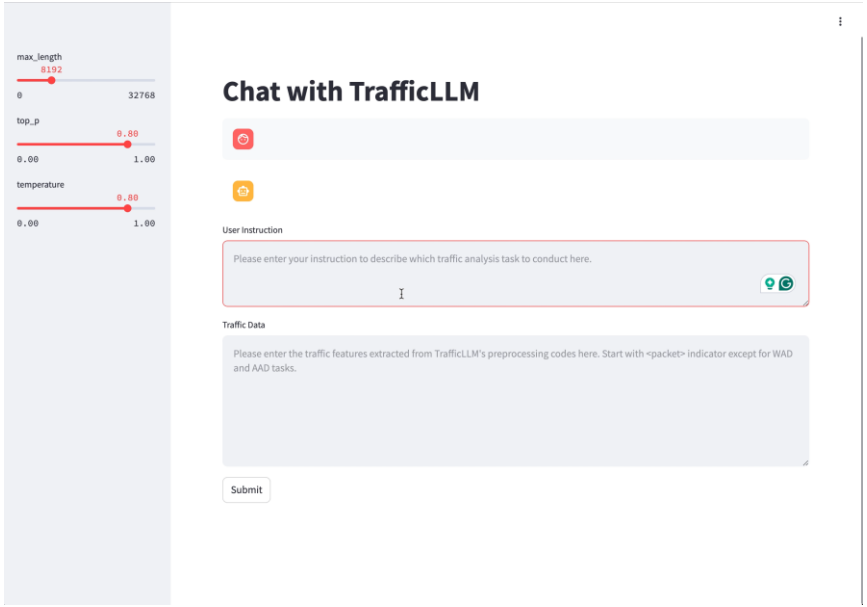
- Based on parameter effective fine-tuning (PEFT) technology, different capabilities are encapsulated in different external parameters.
- Maintain the PEFT model set, with 7.1MB for each external parameter.
- **Advantage:** 69.9% GPU resources and 88.8% training time reduction.



What Got Done

- TrafficLLM has evaluated under 10 downstream tasks, such as Botnet Detection, Malicious DoH Detection, and Web Attack Detection.





ChatBox

Wrap Up

Team members:

- Tianyu Cui, cuity@zgclab.edu.cn
- Xinjie Lin, linxj@zgclab.edu.cn
- Sijia Li, lisj@zgclab.edu.cn
- Prof. Qi Li, qli01@tsinghua.edu.cn
- Prof. Ke Xu, xuke@tsinghua.edu.cn
- Zhongguancun Laboratory & Tsinghua University

Codes

- https://github.com/ZGC-LLM-Safety/TrafficLLM

Papers

- https://arxiv.org/abs/2504.04222

Datasets

- https://drive.google.com/drive/folders/1RZAOPcNKq73-quA8KG_lkAo_EqlwhlQb

Models

- https://drive.google.com/drive/folders/1YjEhdordqZRpnw_oKczwUztcT52T0oQ0

Thank You!

TrafficLLM Homepage

TrafficLLM: Enhancing Large Language Models for Network Traffic Analysis

March 14-20, 2026

Shenzhen, China

IETF